SECUREPOINT
SECURITY SOLUTIONS

Administration Manual

Securepoint Unified Mail Archive

Securepoint Unified Mail Archive, Release 1.0.0.0

Securepoint GmbH, Lüneburg
Security Solutions

SECUREPOINT

Revision Notification

Revision	Release Date	Chapter	Changes
1.0	19.03.2012	all	creation
1.1	01.07.2012	6.5 10 11	update to UMA version 1.0.3 and addition

Content

1 Introduction 6

2 Positioning of the UMA in the Internal Network 7

2.1 Scenario HUB Modus 7

2.2 Scenario Transparent Mode 8

2.3 Scenario Forward Mode 9

3 First-Time Operation 10

3.1 Customize the IP Address 10

4 Connect the UMA Appliance 11

4.1 Direct Connection 11

4.2 Connection Over the Network 12

5 Tab Status 15

6 Lead Tab Setup 16

6.1 Tab Network 16

6.1.1 Network Address Settings 16

6.1.2 Local Name Settings 17

6.1.3 Nameserver Settings 17

6.1.4 Proxy Settings 18

6.2 Tab License 19

6.3 Tab Mail Server 20

6.3.1 Remote Mail Server Settings 20

6.3.2 Remote Smarthost Settings 21

6.3.3 Remote Mail Accounts 21

6.4 Tab Archive Storage 22

6.4.1 Local Storage Integration 22

6.4.2 Network Backup Storage 23

6.4.3 External USB Backup Storage 24

6.5 Tab Accounts 25

6.5.1 User Repository 25

6.5.2 Windows Domain Membership Settings 26
6.5.3 Account Selection 27
6.5.4 LDAP Search Settings 28
6.5.5 Local Users 28
6.5.6 Add User 29
6.5.7 Import CSV File 30
7 Lead Tab Administration 31
7.1 Tab Users 31
7.2 Tab Time 32
7.3 Tab Webmailer / IMAP / SMTP 33
7.3.1 Webmail Access 33
7.3.2 IMAP Server Settings 33
7.3.3 Webserver Certificate / IMAP Certificate / SMTP Certificate 33
7.3.4 Generate Self-Signed Certificates 34
7.4 Tab Indexer 34
7.5 Tab Mail Archive Rules 35
7.6 Tab Backup 36
7.7 Tab Restore 37
7.8 Tab Maintenance 38
7.9 Tab Tools 40
7.10 Tab Logs 41
8 UMA E-Mail-Client 43
8.1 Login 44
8.2 Overview 45
8.3 Folder List 46
8.4 E-Mail Filter 46
8.5 Searching 48
8.5.1 Quick Search 48
8.5.2 Advanced Search 49

8.6 Copy E-Mails 49
8.7 Display an E-Mail 50
8.7.1 Navigation in Displayed E-Mails 51
8.8 Inspection Report 52
9 Auditor Access 53
9.1 Login as Auditor 54
10 Change the IP Address in Windows 7 56
11 Create a HUB E-mail Account on a MS Exchange Server 57
11.1 Define Authentication Method of the IMAP Server 57
11.2 Change the Start Type of the Service 58
11.3 Exchange Management Console 60

1 Introduction

PLEASE NOTE:

This documentation is based on the regulations of German law. Please look after the terms of regulation, which is valid in your country!

This Manual is made for the technicians, which install and configure the Unified Mail Archive (UMA) software or appliance. This Manual has four chapters. The prologue takes care of the setup. Part One describes the administration center; part two explains the e-mail-client and the affix are found in chapter three.

Important information:

We have chosen the terms *archive* and *archiving* very deliberately. We did not make a specific difference between *storage* and *archiving*. It is the opinion of the writers, that users call the storage of documents, which is regulated by law, mostly *archiving*. You find a short definition between *storage* and *archiving* in the affix.

Generally the standard software Securepoint Unified mail Archive (UMA) is offered with a hardware appliance. If an appliance solution is mentioned in this document, this statement is also valid for the software solution. The hardware appliance can get assembled with multiple hard drive disks and in this way it offers in combination with a software RAID controller or an integrated hardware RAID a high level of data security. In dependency of the amount of available hard drive disks the highest possible RAID level is chosen.

The UMA archives the entire e-mail-transfer with a high degree of transparency automatically on a central system. E-mails are saved legally compliant and unchangeable. The Data are saved encrypted on the system and additional a qualified daily time stamp confirms, that no changes on the documents are made during the storage time. All mails, which come through the UMA are going to be saved in copy. Due of this, mails, which are deleted on the e-mail server or on the e-mail client can be reactivated out of the archive.

2 Positioning of the UMA in the Internal Network

You have got several options to integrate the UMA into the existing network. The employment depends on the used e-mail receive and send method.
Following three scenarios are possibly. All scenarios suppose that a mail server is carried on the internal network. It is used for receiving and sending external mails, sending internal mails and dispersing mails in the internal network.

2.1 Scenario HUB Modus

The UMA is not physically positioned in front of the mails server as in the other scenarios. The appliance is connected as server into the internal network.
The e-mails will not be conducted over the UMA. The UMA fetches the e-mails form the mail server.
A HUB account has to exist on the Exchange server. This account contains a copy from every received and sent e-mail. E-mails which are sent over the MAPI interface will be copied into this account. In this way all e-mails will be archived by the UMA.

You can also copy already existing e-mails into the HUB account. When the UMA connects the Exchange server the e-mail stock will be archived.

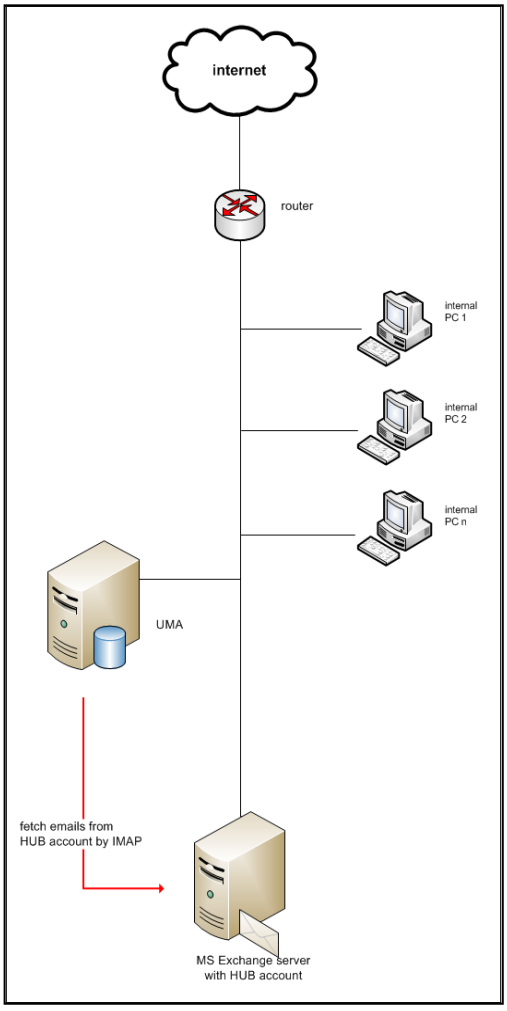

fig. 1 HUB mode

Note:
The preservation of probative value for later archived e-mails begins at the date of the import. Possible probative value loss which occurred **before** the import into the UMA will remain.

2.2 Scenario Transparent Mode

E-mails arrive by SMTP at the router and will be hand on the mail server. Thereby the e-mails pass the UMA.
E-mails, which are sent from the internal network into the internet, pass the UMA on the way to and from the mail server. The same applies for e-mails inside of the internal network.
Thereby all e-mails will be stored by the UMA.

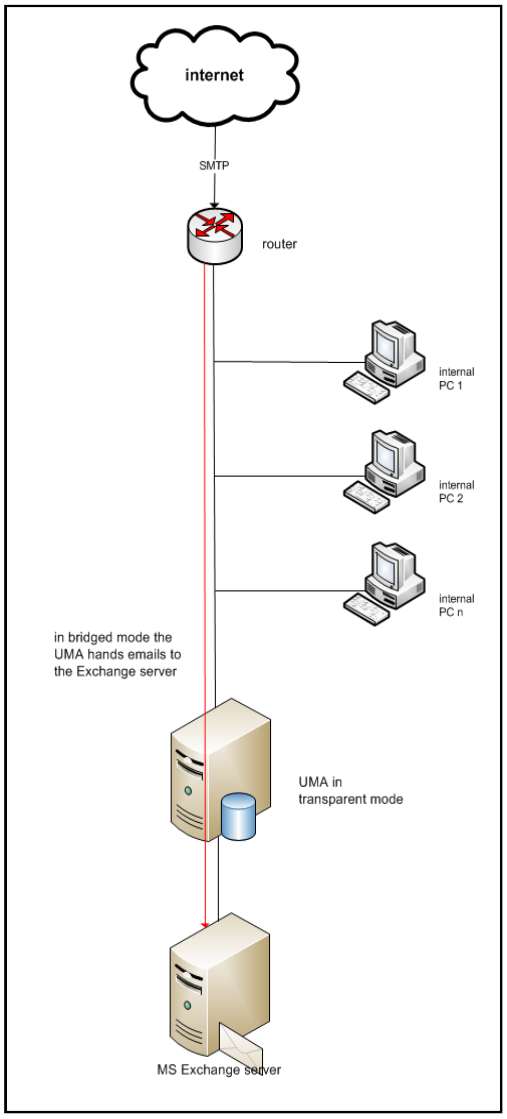

fig. 2 transparent mode

Note:
If the internal computers of the network use the e-mail client Microsoft Outlook and if the mail server is a Microsoft Exchange server, e-mails from these clients will not be stored by the UMA. This combination of mail server and mail client uses the Microsoft specific message architecture MAPI with an RPC protocol.

To archive e-mails which uses this constellation, use the HUB mode (see chapter 2.1).

2.3 Scenario Forward Mode

In this scenario the UMA appliance is also positioned between router and mail server. The UMA fetches e-mails from an external e-mail provider. For this the protocols IMAP, POP3 and others[1] can be used.
The fetched mails will be archived and hand to the mail server.
The dispatch operates identically. E-mails reach the internal mail server which hand them to the UMA. The UMA sends the e-mails to the external provider services by SMTP.

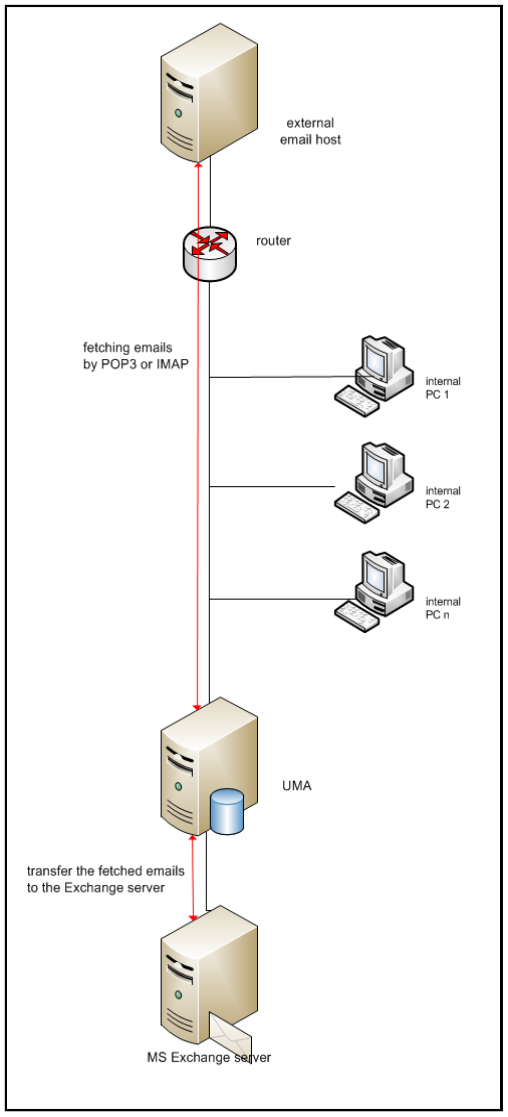

fig. 3 forward mode

Note:
If the internal computers of the network use the e-mail client Microsoft Outlook and if the mail server is a Microsoft Exchange server, e-mails from these clients will not be stored by the UMA. This combination of mail server and mail client uses the Microsoft specific message architecture MAPI with an RPC protocol.
To archive e-mails which uses this constellation, use the HUB mode (see chapter 2.1).

[1] Further protocols can be used: POP2, APOP, RPOP, KPOP, SDPS, ETRN, ODMR

3 First-Time Operation

Some settings are predefined in delivery status. This includes the IP address and the administrator access.

Predefinitions:

IP address: `192.168.175.254`
Subnet mask: `255.255.255.0`
User name: `admin`
Password: `insecure`

3.1 Customize the IP Address

To integrate the UMA appliance into your existing network, you have to adjust the IP address of the appliance. You have got two possibilities: a “direct connection” or a “network connection” by the web interface.
Attach a monitor and a keyboard to the UMA appliance and configure it before your connect it with your network.
You can also configure the appliance within the network. This is only possible if the IP address 192.168.175.254 is used only once in the network; in fact by the UMA appliance. To establish a connection to the UMA it is needed that the computer, you use for the configuration, has an IP address from the same subnet as the UMA appliance (192.168.175.1 – 192.168.175.253). If you need further information how to change the IP address of your computer under MS Windows 7, read the according note in the appendix (see chapter 10).

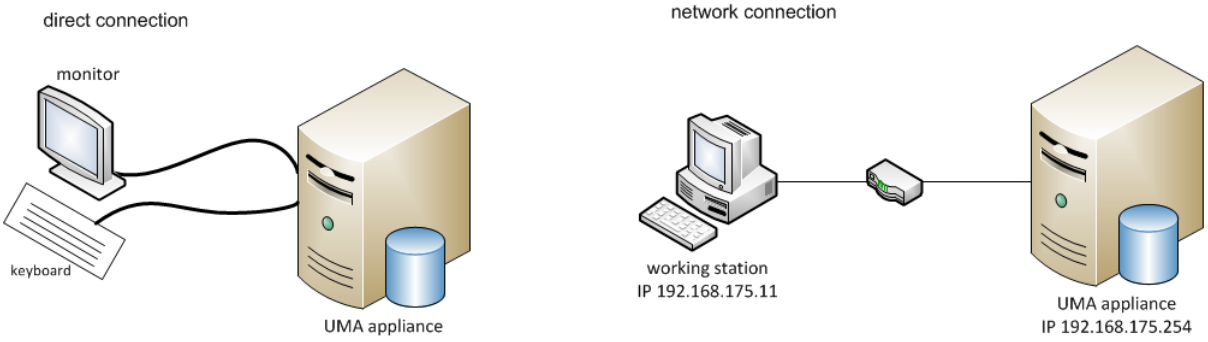

fig. 4 connection to the UMA appliance to configure the IP address

4 Connect the UMA Appliance

4.1 Direct Connection

The direct connection with monitor and keyboard is only destined to change the IP address temporary and prepare the appliance for the employment in the network without changing the IP address of your work station.

Login the UMA appliance with the predefined administrator account.

login: `admin`

password: `insecure`

You are logged in as user with restricted super user rights.
In delivery status the appliance adjusts a connection in transparent mode. The entire network traffic will be routed over the UMA appliance. The appliance only attends to the e-mail traffic. All other data packets will be passed through.

Change the IP address of the UMA appliance with the following command.

ip addr replace	192.168.100.10/24	**dev**	bridge0
command	new IP address with bitcount		interface

In this example the network uses the subnet 192.168.100.0/24.

Note:
The command changes the IP address just temporally. The address will not be stored and will reset to delivery status when the appliance will be rebooted. For permanent saving you have to change the IP address over the web interface.

After the IP address is adjusted to the network subnet, you can open the **UMA-Administration-Center** in your web browser.

4.2 Connection Over the Network

- Open your web browser. Enter the new UMA IP address into the browser's address bar. You have to use the HTTPS protocol and the port 11115.

  `https:///192.168.100.10:11115/`

- The web interface uses a self-signed certificate, which will be classified as an un-trustworthy website. Therefore a security warning appears.
  Confirm that you trust the supplier of the certificate.
  The certificate can be exchanged with an own one later, which will be classified trustworthy in the network (see chapter 7.3.3).

- The login screen of the UMA-Administration-Center appears.

- Enter the credentials of the predefined default admin.

  user name: `admin`

  password: `insecure`

fig. 5 login screen

Note:
Remember to change the password as soon as possible.
This function is described in chapter 7.1.

Note:
A secure password has a length of minimum 8 characters. It should be a random combination out of lower case, upper case, numeric and special characters.

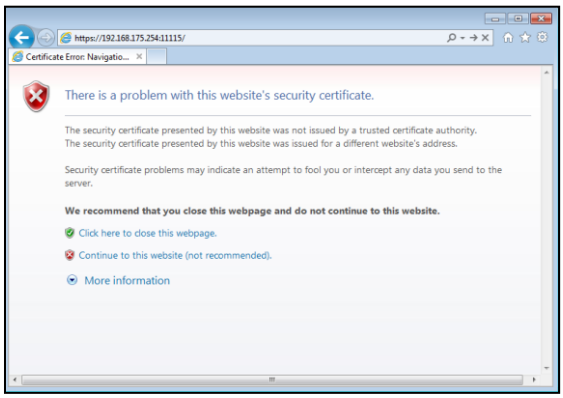
There is a problem with this website's security certificate.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

fig. 6 security warning MS Internet Explorere

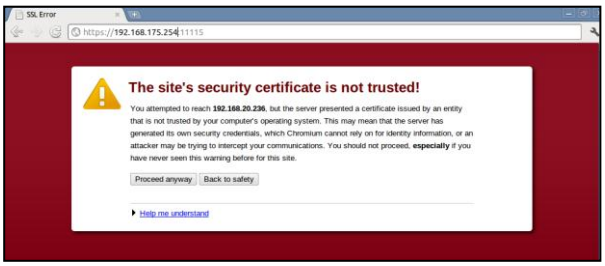

fig. 7 security warning of Google Chrome

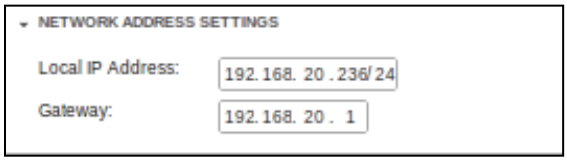

fig. 8 set new IP address

- Enter the new IP address of the UMA appliance at the UMA-Administration-Center.
  Switch to the tab **Setup/Network**, **Network Address Settings**.
  Enter the new IP address into the field **Local IP Address** (for example 192.168.175.20).
  Click on **Save**.
- The IP address will be stored permanently in the configuration file.

Part 1

UMA Administration Center

5 Tab Status

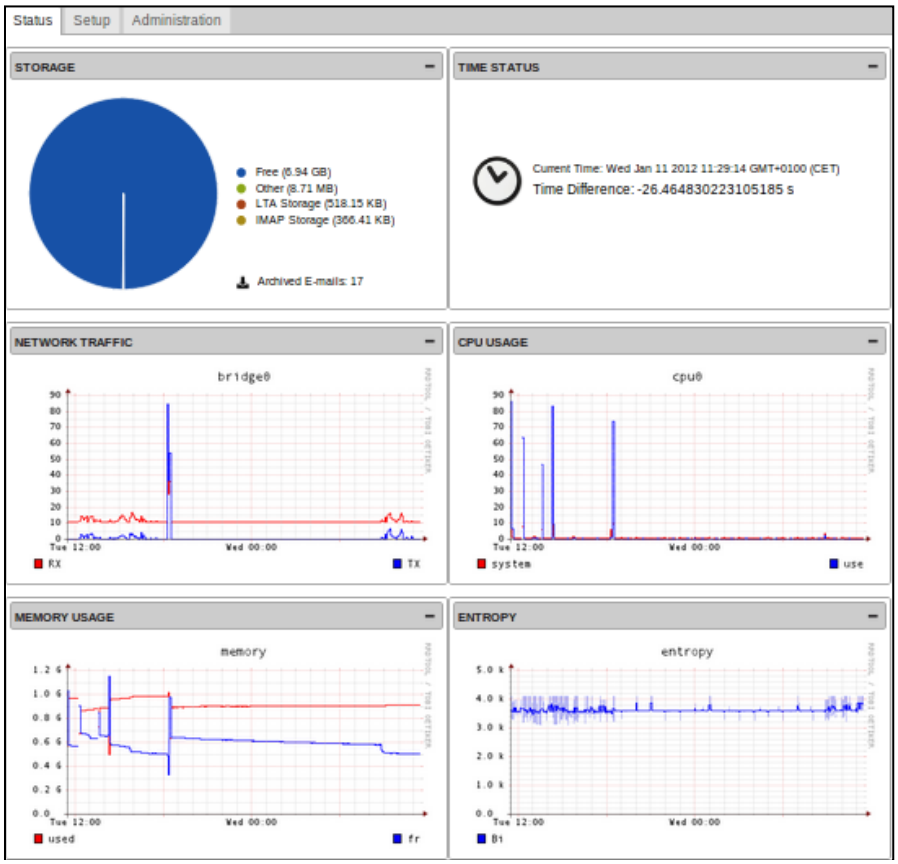

fig. 9 first shown screen after login

The tab **Status** appears after login. It shows system information graphically.
The area **Archive Storage** shows the available memory capacity and the used storage space according to several directories. Furthermore the numbers of archived e-mails is shown.

Note:
The storage is not initialized and no e-mail is archived at initial operation. So no information can be shown. The display will be refreshed hourly.

The area **Time Status** shows the current time and the difference between system time and the called time from the time server. This information will be shown when the time server is defined and accessible.
The displayed graphs show the hardware utilization.

Note:
The system time has no influence to the probative value. This is only bound to the qualified timestamp.

6 Lead Tab Setup

At the initial startup of the appliance you have to define general settings.
The first configuration steps are summarized under this tab.

6.1 Tab Network

On the tab Network several settings of the environment are subsumed.

6.1.1 Network Address Settings

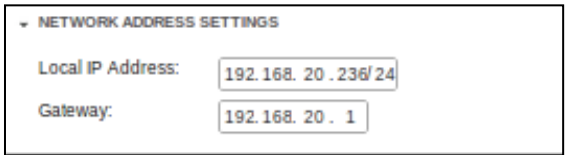

fig. 10 set the appliance IP and the Gateway IP

- Define the desired IP address of the appliance in the area **Network Address Setting**.
  The declaration expects a bit count which defines the network subnet.
  Click on **Save**. The button appears behind the input field after typing.
- After this changing the appliance is only reachable under the new IP address. You have to login again.
  Enter the **new IP address** of the appliance into the address bar of your browser followed by a **colon** and the port **11115**.
  Use the **HTTPS** protocol: `https://newAddress:11115/`
  Confirm that you trust the certificate issuer and login with the default administrator account.

Note:
If you change the password already, use the new password for login.

- Enter the IP address of your internet access device into the field **Gateway**.
  Click on **Save**.

6.1.2 Local Name Settings

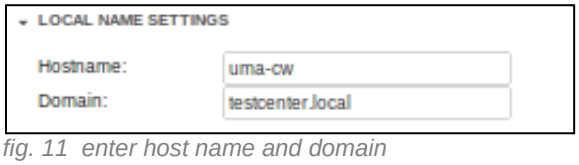

fig. 11 enter host name and domain

- Enter a host name for the appliance into the field **Hostname** and the domain of your network into the field **Domain**.
- Click on **Save**.

6.1.3 Nameserver Settings

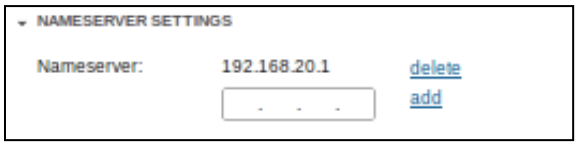

fig. 12 enter DNS server IP addresses

- Enter the IP address of your nameserver in the section **Nameserver Settings** and click on **Add**.
  If you use more than one nameserver, repeat this procedure till al nameserver are added. You can define three nameserver.

6.1.4 Proxy Settings

If you use a proxy in your network, define the settings the appliance needs to establish a connection to the internet.

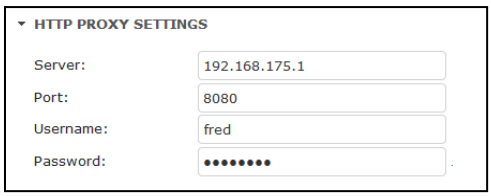

fig. 13 proxy credentials

- Enter the hostname or the IP address of proxy server into the field **Server**.
- Type the port the proxy works on into the field **Port**.
- The credentials the UMA appliance should use for authentication have to be defined in the fields **Username** and **Password**.

Note:

The UMA only supports the “Basic Authentication”.

Now the general network settings are made.

6.2 Tab License

To use all functions and features of the UMA you have to import a license. A license can be purchased from the Securepoint GmbH or from your reseller.

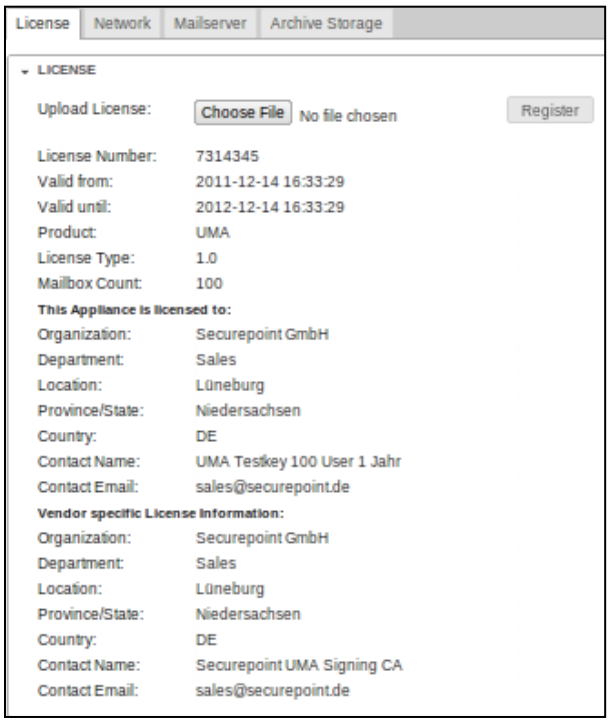

fig. 14 example for a license

- Switch to the tab **License** under the lead tab **Setup**.
- Click on the button **Choose File** and select the license file in the file dialog from the files system of your computer.
- Click on the button **Register**.

If the file is installed, you can set further settings.

Note:

The license file can only be placed at the disposal, if the document “Unterrichtung gemäß § 6 SigG mit § 6 SigVo betreffend Leistung von akkreditierten Zeitstempeldiensten” is signed by the owner of the UMA appliance and sent back to the Securepoint GmbH.

The document is available under following URL *https://my.securepoint.de* in the reseller portal.

6.3 Tab Mail Server

On this tab you have to define the settings of internal and external mail server.

6.3.1 Remote Mail Server Settings

Enter here the settings of the mail server of your internal network. If you use the HUB mode, you have to define the domain you want to retrieve mails from. Furthermore you have to define the connection data to the mail server where the HUB account is hosted. This is described in the chapter **Remote Mail Accounts** (see chapter 6.3.3).

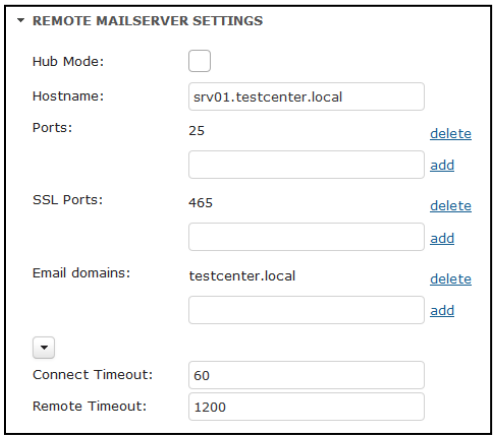

fig. 15 mail server settings for the Transparent and Forward Mode

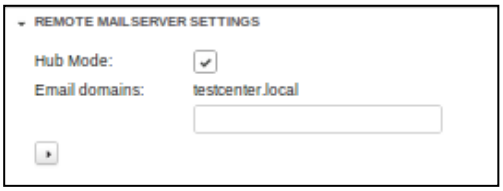

fig. 16 mail server settings for the HUB mode

Area / Field	Description
Hub Mode	Activates the HUB mode. A HUB account must have been defined on the mail server which includes a copy of every mail.
Hostname	Declaration of the hostname or IP address of the mail server.
Ports	Declaration of the ports the mail server sends mails by SMTP.
SSL Ports	Declaration of the SSL secured SMTP ports of the mail transport.
E-mail domains	Declaration of the domains which are managed by the server.
Connect Timeout	Define the maximum time for a connection attempt.
Remote Timeout	Define the maximum time for an active connection.

6.3.2 Remote Smarthost Settings

Apply these settings if you use a mail relay (of a provider) for the mail transport or if your firewall expects an authentication for the SMTP protocol.

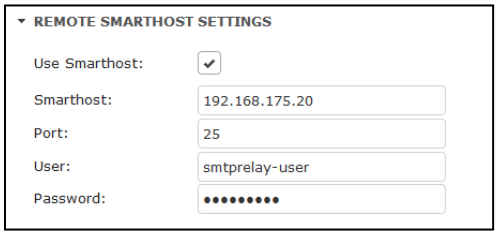

fig. 17 settings for a remote mail relay or SMTP authentication

Area / Field	Description
Use Smarthost	Activates the smarthost function.
Smarthost	Hostname or IP address of the smarthost.
Port	SMTP port of the smarthost.
User	User name of the host account.
Password	Password of the host account.

6.3.3 Remote Mail Accounts

Define these settings, if you fetch mails from e-mail accounts hosted by an external provider. If you use the HUB mode, you have to configure the credentials to the mails server and the HUB account in this section.

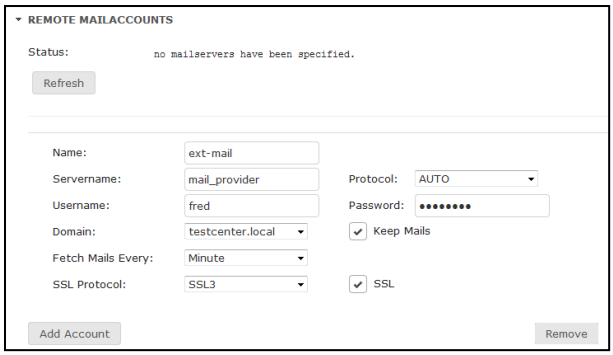

fig. 18 mail accounts on an external server

Area / Field	Description
Status	Shows the notifications of the last retrieve.
Refresh	Starts a new retrieve immediately.
Name	Define a name for the external account.
Server Name	Declaration of the hostname or IP address of the e-mail server.
Protocol	Selection of the used protocol (for example POP3, IMAP).

Area / Field	Description
Username	Declare the username of the mail account.
Password	Declare the password for the mail account.
Domain	Declaration of the domain which is managed by the provider.
Keep Mails	Decide if the mails should be left on the server.
Fetch Mails Every	Define the interval for the automatically retrieve of the mails.
SSL Protocol	Select the SSL encryption method.
SSL	Activates the SSL encryption.
Add Account	Opens an entry mask for a new account.
Remove	Deletes the account settings.
Save	Saves changes of the settings.
Revert	Resets the settings.

Note:

Usually is sufficient to set the protocol selection to **AUTO**.

6.4 Tab Archive Storage

The storage for the e-mail archive will be initialized under this tab. Furthermore settings of the backup function will be defined. The backups could be saved on network storage or an USB device.

6.4.1 Local Storage Integration

The e-mail archives will be stored on the local hard disc drives of the appliance. The drives are conducted in a RAID system. Depending on the accouterment of the appliance this is managed by a software or hardware RAID controller.
If a software RAID controller is used, the correct RAID level will be selected automatically.
At the initial startup of the appliance the archive storage has to be initialized first. For this click the Button **Initialize**.

6.4.2 Network Backup Storage

You can create backups of the archive storage and save them on the network. For this the UMA appliance offers three types of network storage. You can transmit the backups to an fileserver via Windows Share (Server Message Block Protocol), via SSH (Secure Shell) or via FTP (File Transfer Protocol).

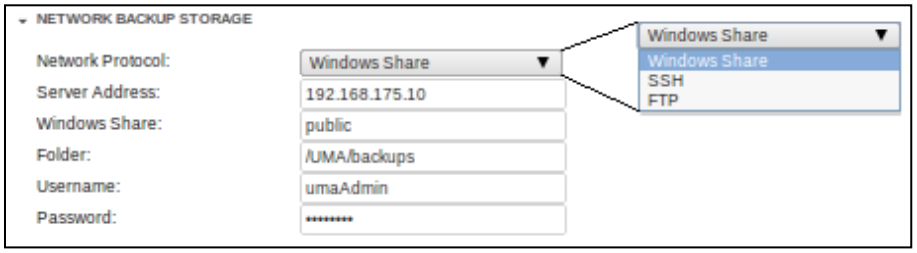

fig. 19 set network storage

Area / Field	Specific Fields	Description
Network Protocol		Select a supported network protocol.
Server Address		Declare the hostname or IP address of the server.
Folder		Directory the backup should be saved in. Don't use directory names with blanks.
Username		User name at the host.
Password		Password of the user at the host..
Windows Share	Windows Share	Declare the public directory of the server.
SSH	Folder (complete path)	Enter the complete path (from root directory) of the storage folders.

6.4.3 External USB Backup Storage

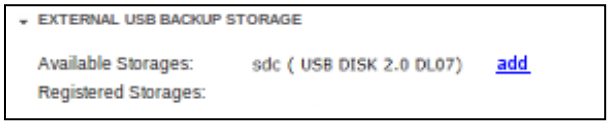

fig. 20 available USB devices

The backups can also be saved on a device which is connected to the appliance by USB. This can be an USB flash drive or an external hard disc drive for example.
Under **Available Storages** all recognized USB storage mediums are shown. Select the desired medium out of the list and click in the according row on **add**.
The medium will be shown under **Registered Storages**.

Attention:

You need a configuration backup of the UMA (see the tab **Maintenance** chapter 7.8), to play back a storage backup from the USB device.

The USB device has to be already registered in the configuration.

A new registration of the USB device will delete all data on the medium.

6.5 Tab Accounts

On this tab you can decide from which source the e-mail accounts information will be received. Furthermore it can be decided which e-mail accounts should be archived by the UMA.

6.5.1 User Repository

You can choose between two types of receiving the account information.
The UMA system can be integrated into a Windows domain. The e-mail accounts can be took from the Active Directory.
The second possibility is to enter the e-mail accounts manually or import them by a comma separated list. (CSV file).

fig. 21 select source

- Select the desired source in the area **User Repository**.
- Choose **Local User** for manually entry or import of a CSV file.
- Choose **Windows Active Directory** to use the Windows directory service.
- According to the selected method the tab will be designed to record the relevant parameters.

6.5.2 Windows Domain Membership Settings

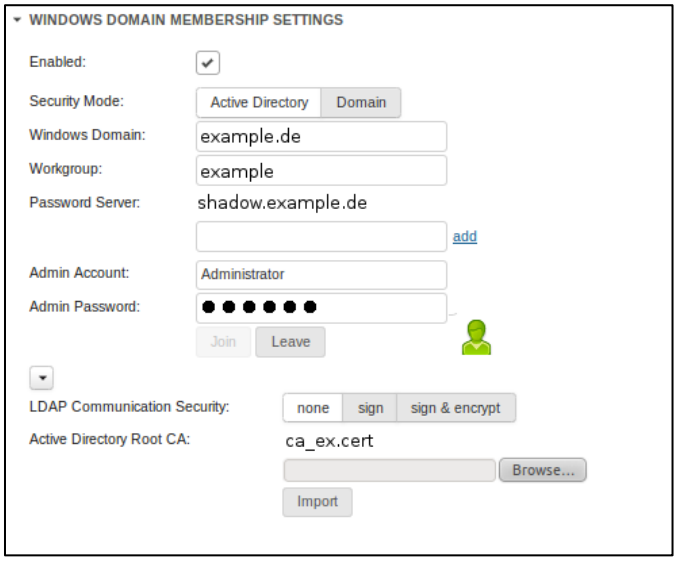

fig. 22 register to a domain

In this section you can decide, to register the UMA appliance at an **Active Directory** or a **Windows Domain**.

- Activate the checkbox **Enable** to unlock the function.
- Select the registration type and click the according button.
- Enter the name of the domain into the field **Windows Domain**.
- Type the name of the group into the field **Workgroup**.
- Enter the hostname or the IP address of the server into the field **Password Server**.
- Enter the administrator credentials into the fields **Admin Account** and **Admin Password**.
- Click **Join**.
  If the registration was successful, the symbol beneath the button becomes green.

Furthermore the **communication security** of the LPDA connection can be set. To open this area click the button with the **arrow** below the buttons **Join** and **Leave**.

- Select the security level of the connection at the row **LDAP Communication Security**.
- To deposit a root certificate (CA) click on **Browse** and select a CA from your system.
- Click on **Import**.

6.5.3 Account Selection

If you do not want to archive all e-mail accounts which are managed by the Active Directory, you can select several e-mail accounts. To use this function you have to be logged in to an Active Directory.

fig. 23 select e-mail accounts

- Activate the checkbox **enable manual select** in the area **Select Accounts To Store**. Two lists with the available e-mail accounts and two search fields appear.
- The left list shows the user e-mail accounts. The right one shows mailing lists.
- You select desired accounts by **activate the checkbox ahead** of the account. The selection will be work immediately.
- An entry into the **search fields** limits the shown accounts. This takes affect by typing only one character.

6.5.4 LDAP Search Settings

The automatic selection of the e-mail accounts from the Active Directory can be limit to a defined area.

For this use the **LDA Search Settings**.

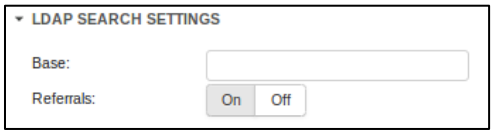

fig. 24 set start point of search

- Define the point the search should begin from. The directory tree will be searched downward.
  Enter this point into the field **Base**.
- If you want to include references in the directory tree, click on the button **On** behind the field **Referrals**.

6.5.5 Local Users

If you selected the option local users, you can archive the e-mail accounts by the UMA without using an Active Directory.

You can enter e-mail accounts manually or import them from a comma separated list. You can also combine both options.

fig. 25 list of local user accounts

- The area **Local Users** offers the options **Add User** (manual input) and **CSV Import**.
- Entered e-mail accounts are shown in a list below.

- An entry into the **search field** limits the shown accounts. This takes affect by typing only one character.
- You can **edit an e-mail account** by clicking on it.
- If an account should be deleted from the list, click on the button **delete** beneath the respective account.

6.5.6 Add User

If you want to add user e-mail accounts manually, click the button **Add User** in the **Local Users** area. The following entry mask appears.

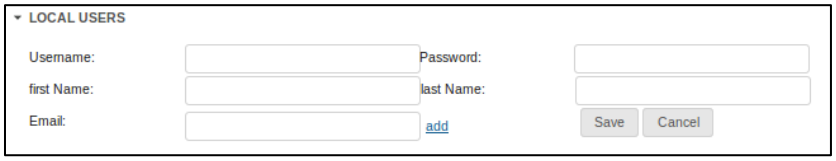

fig. 26 add users manually

- Enter the queried data.
- Type the e-mail account password into the field **Password**.
- If you want to enter more than one e-mail address click the button **add**. Another field **E-mail** appears.
- Store the entry with the button **Save**.
- If you click **Cancel**, the mask will be closed without saving the data.

6.5.7 Import CSV File

You can also import an e-mail account list. This must be given in CSV format. Following information are necessary for a successful import:

account name,password,first name,last name,e-mail address,optional e-mail address

The whole list is set into quotation marks.

Example:

```
"fredf,secret,Fred;Flintstone,fred@flintstone.tv,fred@flintstone.com
 donald,topsecret,Donald,Duck,donald@duck.com"
```

fig. 27 import mask

- Click on **Browse**… to select a CSV file from your system.
- Click on **Import**. If the import process was successful the updated list appears.

7 Lead Tab Administration

7.1 Tab Users

On this tab the system users will be declared. These users configure the system and can manage mailboxes.
“Normal” users, which use the UMA-E-mail-Client interface don’t have to be declared, because they will be authenticated by the Active Directory.

Note: DyUDe (Dynamic User Detection)

Mailboxes will be created dynamically. The UMA appliance automatically creates archive mailboxes if an e-mail is sent or an e-mail is received.

The UMA generates a mailbox per user when the users receives or sends e-mails. The number of mailboxes is limited by the license. If the license allows five mailboxes, e-mails will be archived for five users. E-mails of remaining users will not be archived.

The e-mail database will be saved in four-eyes-mode. Inspection of user mail account by other persons is only allowed for an auditor if the privacy officer authorizes the access. After the auditor has logged on to the e-mail-client web interface the privacy officer has to log in to approve the access.

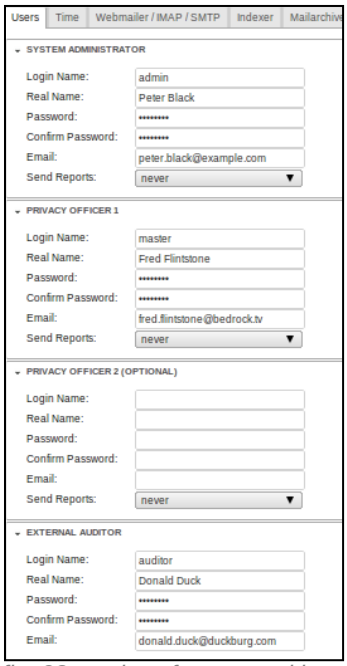

fig. 28 settings for users with special rights

Area / Field		Description
System Administrator Privacy Officer 1 Privacy Officer 2 External Auditor	Login Name	Declare the user name for the web interface.
	Real Name	Enter the first and the last name of the user.
	Password	Define the password of the user.
	Confirm Password	Confirm the password by retype the password.
	E-mail	Enter the e-mail address of the user.
Send Reports for administrator and privacy officer	daily weekly monthly never	Reports will be sent in the selected interval.

7.2 Tab Time

Here you have to set the time of the appliance. The appliance obtains the time from a time server in the internet or in the internal network. By defining the time zone the time is adjusted to the desired time zone.

Note:

This setting isn't importing for the qualified timestamp (QTS). Only the QTS are relevant for the judicial probative value of the e-mails.

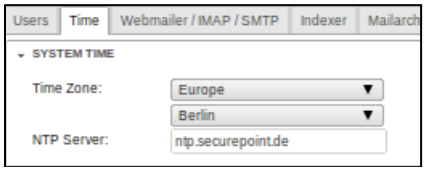

fig. 29 select time zone and time server

Area / Field		Description
Time Zone	(sub) continent	Select the continent the appliance stands.
	city	Select the city which is placed in the same time zone.
NTP Server (Network Time Protocol)		Enter the hostname or the IP address of a server which publishes the current time.

7.3 Tab Webmailer / IMAP / SMTP

On this tab the security settings like certificates and encryption of the server services are defined.

7.3.1 Webmail Access

This activates the UMA-E-Mail-Client which is reachable under the internal address of the UMA appliance.

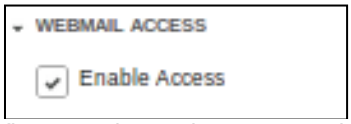

fig. 30 activates the access to the e-mail client

7.3.2 IMAP Server Settings

Define if the IMAP server uses SSL encryption and which user authentication type should be used.

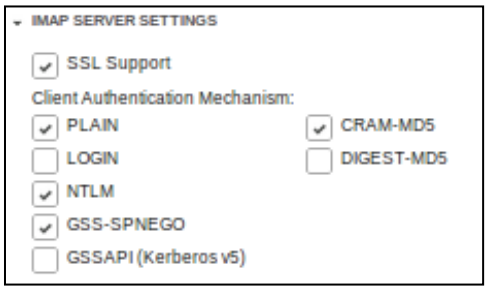

fig. 31 define IMAP encryption and authentication

7.3.3 Webserver Certificate / IMAP Certificate / SMTP Certificate

These areas show information of the used certificates of the webserver, the IMAP server and the SMTP server.
In delivery status the appliance uses self-signed certificates. For security reason web browsers warn the user to open internet sites, which use a self-signed certificate.
You can import a certificate. This can be an own one or a certificate from an official trusted certification center. If you use a self-signed certificate you have to deposit the root certificate (Certification Authority CA) at the domain controller as a trustable root certificate.

fig. 32 certificate of the webserver

fig. 33 certificate of the IMAP server

fig. 34 certificate of the SMTP server

7.3.4 Generate Self-Signed Certificates

To set the appliance back to delivery status, you can generate a self-signed certificate by the appliance.

fig. 35 generate self-signed certificate

7.4 Tab Indexer

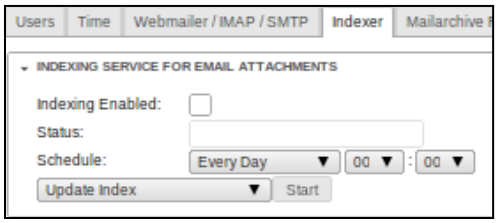

fig. 36 attachment indexer

This function indexes e-mail attachments of the archived e-mails. This accelerates the search.

The indexing can be executed as a schedule. The index can always be rebuilt or continued.

Note:

The indexing accelerates the access on the content of the attachments. This procedure takes up disk drive space. The size of the extra required disk space is depending on the size, the type and the format of the attachment.

7.5 Tab Mail Archive Rules

On this tab you can define rules which will be used to assign the e-mails to the archives **6 years**, **10 years**, **30 years** and **forever**.

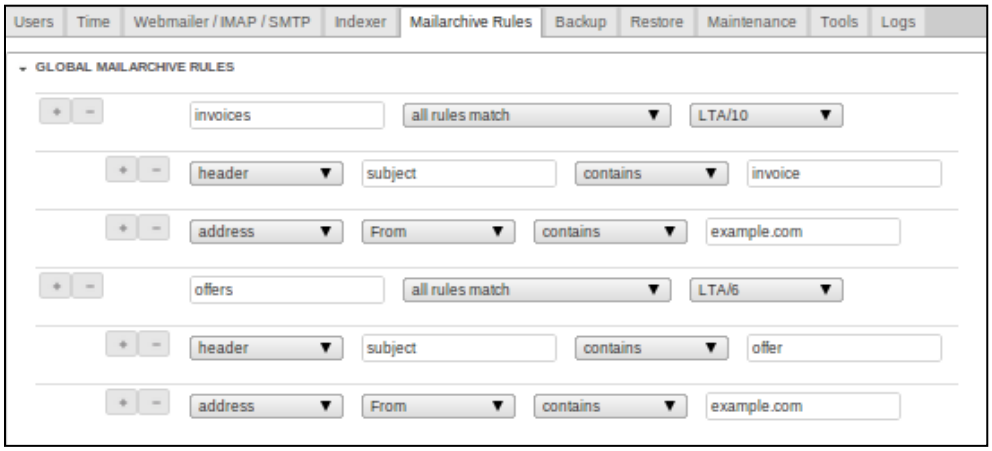

fig. 37 rule table

To set up a filter condition you have to enter a name for this rule first. Than you select the match conditions and the archive the matching e-mails should be copied to.

Match of conditions:

- **all rules match**
- **one rule matches**
- **no rule matches**

Following sections could be searched:

- **e-mail header**
- **e-mail body**
- **address**
- **body**

In dependency on the sections different conditions can be selected.

Section	Condition 1	Condition 2
e-mail header	subject / date	contains / matches / is
e-mail body	raw / content / text	contains / matches / is
address	to / from / carbon copy (CC)	contains / matches / is
size	greater than / less than	K / M / G (kilobyte / megabyte / gigabyte)

Note:

Settings made on the tab **Mail Archive Rules** are global and have effect on all mailboxes.

Furthermore, the user can set filter which copy desired e-mails into archive folders with longer archive time (see chapter 8.4).

The global rule set is super ordinate.

7.6 Tab Backup

You can back up the whole system weather on network storage or onto an external medium. Both backup possibilities are combinable.

The network storage has to be defined in the menu **Setup** on the tab **Archive Storage**.

External storage medium have to be connected to the appliance by USB port. External hard disk drives and flash devices are supported. These external devices have to be registered in the menu **Setup** on the tab **Archive Storage**.

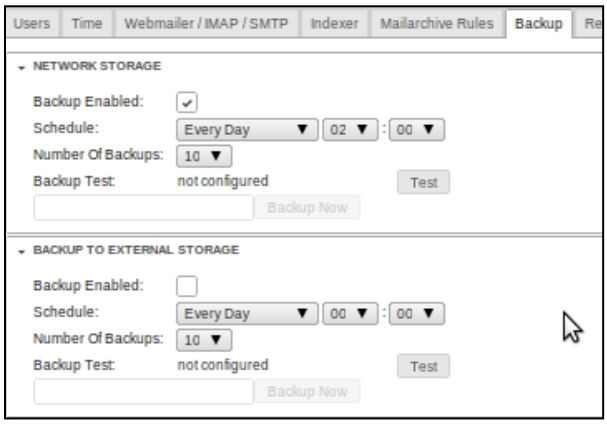

fig. 38 activate and schedule backup

Area / Field	Description
Backup Enabled	Activates the automatic backup routine.
Schedule	You can select the day of the week and the time. Besides, the values workday and every day are offered.
Number Of Backups	Defines the number of stored backups. If the value will be exceeded the oldest backup will be deleted.
Backup Test	Tries to establish a connection to the storage medium.
Backup Now	Creates a backup instantly.

7.7 Tab Restore

The functions on this tab restore saved backups. The restore is available from network storage or external medium.
Saved backups are shown in the dropdown field **Available Backups**.

The name of a backup is composed like this:

`uma-backup-YYYY-MM-DDTHH-MM-SSZ+TZD.tar.gz`

`YYYY` year four-digit

`MM` month two-digit

`DD` day two-digit

The following `T` stands for Tag (day).

`HH` hour two-digit

`MM` minute two-digit

`SS` second two-digit

The following `Z` stands for Zeit (time).

`TZD` time zone difference four-digit

The prefix (+/-) shows if the defined hours must be added or subtracted to/from the Universal Time Coordinated (UTC).

Refresh reloads the backup list.
Restore installs the selected backup.

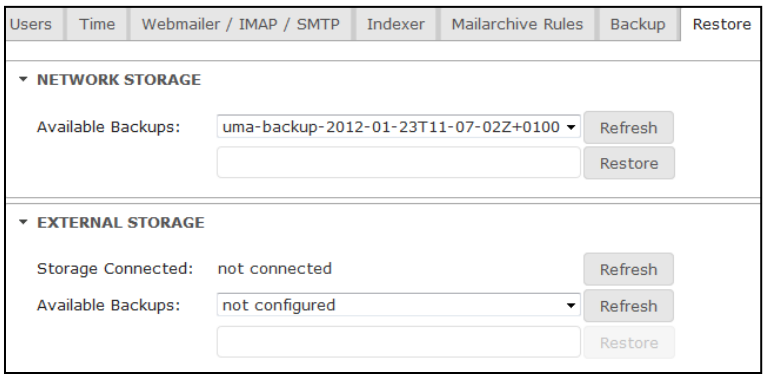

fig. 39 restore backup

7.8 Tab Maintenance

In this section you can execute basic management tasks.

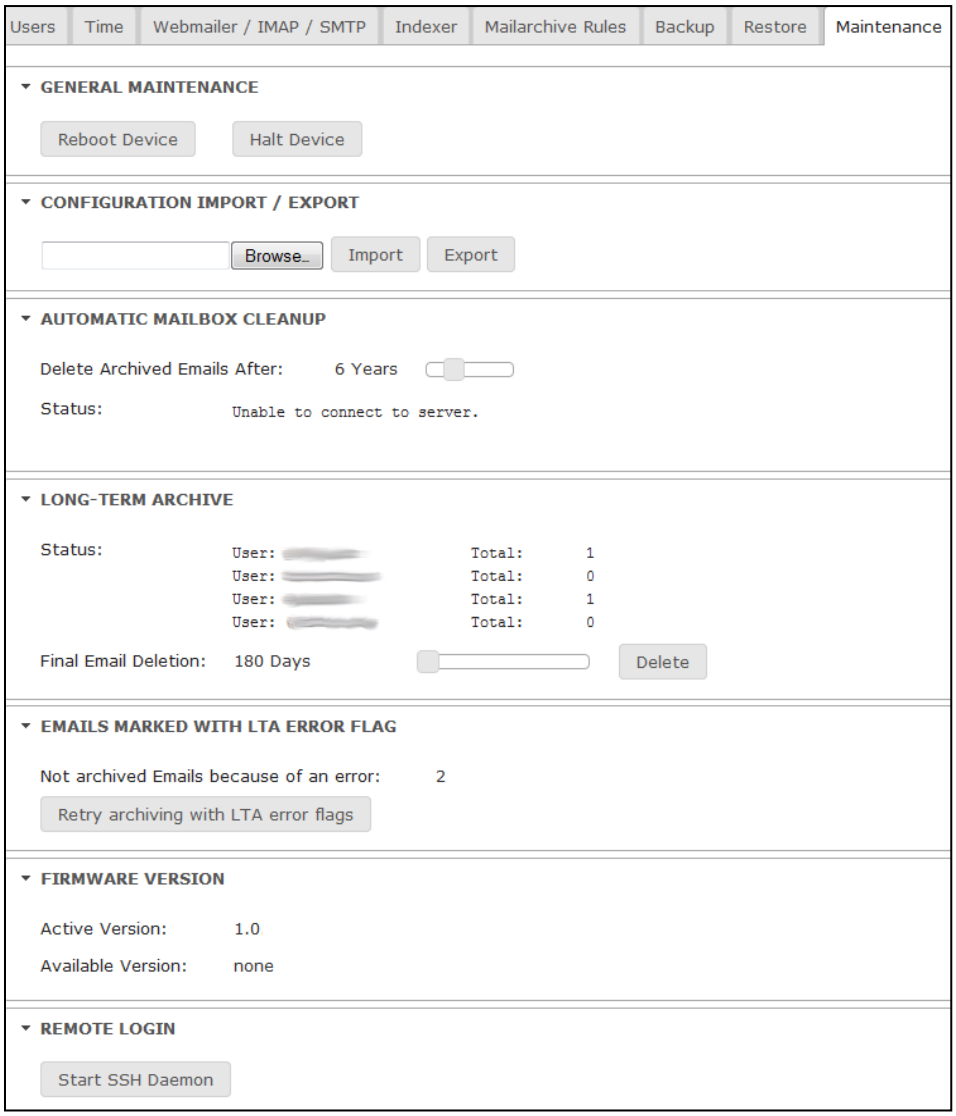

fig. 40 maintenance functions

Area / Field		Description
General Maintenance	Reboot Device	Restarts the system.
	Halt Device	Shuts down the system.
Configuration Import / Export	Choose File	Opens a dialog to search a configuration file on the local system.
	Import	The selected file from the local system will be imported to the appliance.
	Export	Exports the current running configuration.
Automatic Mailbox Cleanup	Slide Control	Use the slide control to set the number of years the e-mails should be saved. E-mails which are older than the adjusted time will be deleted.

Area / Field		Description
		The values are selectable between 1 and 20 years and never.
	Status	Shows which mailboxes are cleaned up.
Long-Term Archive	Status	Shows a warning which mailboxes and how many e-mails will be affected by a deletion. Only e-mails which have reached the storage time will be deleted.
	Slide Control	If e-mails have exceeded the long term archive duration they will be held back before definitely deletion. With this control the hold back time can be set between 180 to 365 days.
E-mails Marked With LTA Error Flags	Not archived e-mails	Shows the number of e-mails which are not archived (caused by an error).
	Retry	Copies the marked e-mails to the LTA at the next archive run.
Firmware Version	Active Version	Shows the version number of the utilized standard software.
	Available Version	Shows the version number of potential updates.
	Download Bandwidth	Limits the bandwidth for the download.
	Changelog	Shows the changes between the current version to the previous version.
Remote Login	Start SSH Daemon	Start the SSH services on the appliance. So you can connect the appliance with an SSH client. For login use following credentials: user name: admin password: insecure This service waits for connection the next ten minutes. If no login occurs in this time the service will be shut down.

7.9 Tab Tools

This tab offers operations which test for example the functionality of e-mail delivery, network availability and hard disk functionality.

Area ./ Field		Description
E-Mail Delivery Test	Host	Enter the host name or the IP address of the mail server which shall send the e-mail.
	E-Mail Address	Enter the address of the recipient of the test e-mail.
	Results	Shows the result of the test.
Network Tools	Tool	You can select between the functions **ping**, **host** and **traceroute**.
	Host / IP	Enter the IP address or the host name of the target system for the test.
	Run	Starts the test.
	Results	Shows the result of the test.
S.M.A.R.T. Hard Drive Test	Schedule	Select a schedule for the hard disk test. The test can be executed monthly, half yearly or yearly.
	Status	Shows the result of the test.

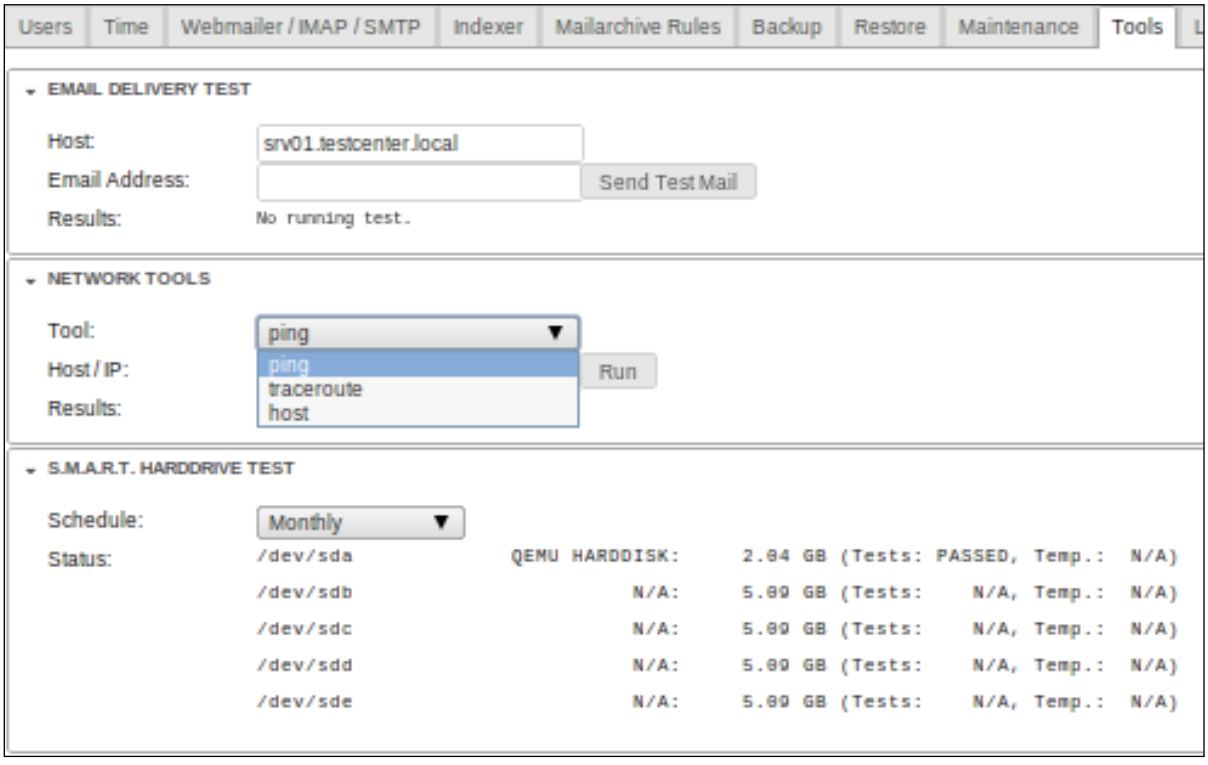

fig. 41 maintenace tools

7.10 Tab Logs

Syslog protocol entries can be saved on the appliance or on an external syslog server.

Area / Field		Description
External Logs	Enable	Activates the sending of protocol entries to an external syslog server.
	Syslog Server	Enter the IP address or the host name of the syslog server.
	Port	Enter the port the syslog server uses (default: 514):
Show Log	Service	Protocol entries can be show ordered by service.
	Fetch Logfile	Loads the desired log entries.
	Filter	Die displayed entries can be filtered. Possible filters are: none (all entries are shown) error (only error messages) warning (only warnings) info (only information messages) debug (only debug messages user defined (User can define the search pattern in the entry field.)
	Filter Button	Starts the filter.
	Reset	Resets the search filter.

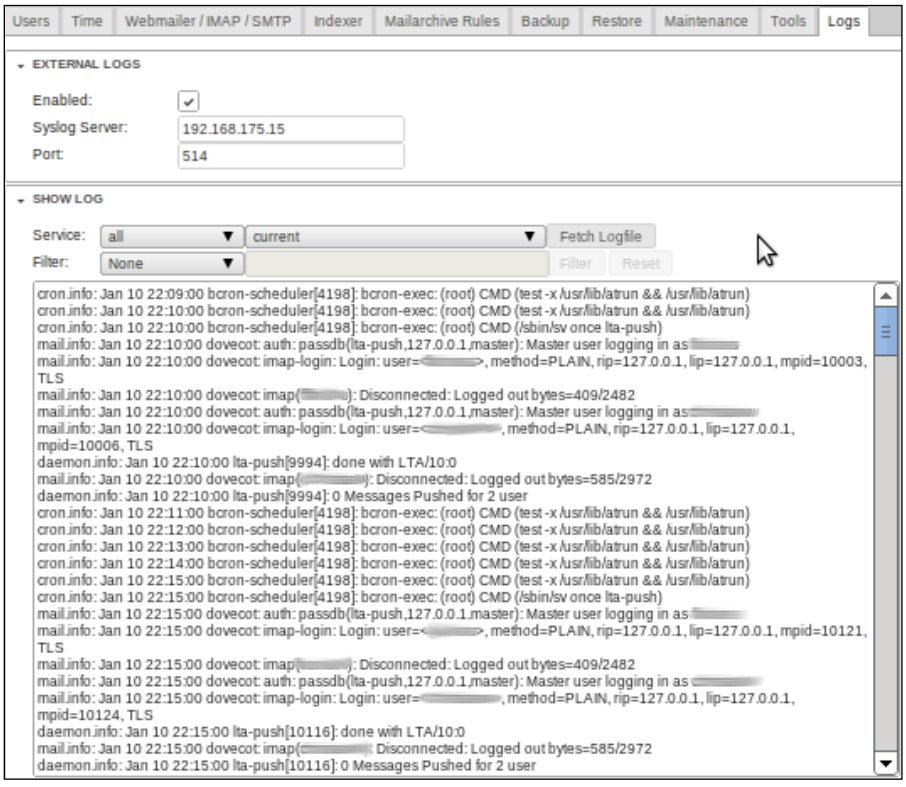
Users
Time
Webmailer / IMAP / SMTP
Indexer
Mailarchive Rules
Backup
Restore
Maintenance
Tools
Logs
EXTERNAL LOGS
Enabled:
Syslog Server:
192.168.175.15
Port:
514
SHOW LOG
Service:
all
current
Fetch Logfile
Filter:
None
Filter
Reset
cron.info: Jan 10 22:09:00 bcron-scheduler[4198]: bcron-exec: (root) CMD (test -x /usr/lib/atrun && /usr/lib/atrun)
cron.info: Jan 10 22:10:00 bcron-scheduler[4198]: bcron-exec: (root) CMD (test -x /usr/lib/atrun && /usr/lib/atrun)
cron.info: Jan 10 22:10:00 bcron-scheduler[4198]: bcron-exec: (root) CMD (/sbin/sv once lta-push)
mail.info: Jan 10 22:10:00 dovecot: auth: passdb(lta-push,127.0.0.1,master): Master user logging in as
mail.info: Jan 10 22:10:00 dovecot: imap-login: Login: user=<, method=PLAIN, rip=127.0.0.1, lip=127.0.0.1, mpid=10003, TLS
mail.info: Jan 10 22:10:00 dovecot: imap(): Disconnected: Logged out bytes=409/2482
mail.info: Jan 10 22:10:00 dovecot: auth: passdb(lta-push,127.0.0.1,master): Master user logging in as
mail.info: Jan 10 22:10:00 dovecot: imap-login: Login: user=<, method=PLAIN, rip=127.0.0.1, lip=127.0.0.1, mpid=10006, TLS
daemon.info: Jan 10 22:10:00 lta-push[9994]: done with LTA/10:0
mail.info: Jan 10 22:10:00 dovecot: imap(): Disconnected: Logged out bytes=585/2972
daemon.info: Jan 10 22:10:00 lta-push[9994]: 0 Messages Pushed for 2 user
cron.info: Jan 10 22:11:00 bcron-scheduler[4198]: bcron-exec: (root) CMD (test -x /usr/lib/atrun && /usr/lib/atrun)
cron.info: Jan 10 22:12:00 bcron-scheduler[4198]: bcron-exec: (root) CMD (test -x /usr/lib/atrun && /usr/lib/atrun)
cron.info: Jan 10 22:13:00 bcron-scheduler[4198]: bcron-exec: (root) CMD (test -x /usr/lib/atrun && /usr/lib/atrun)
cron.info: Jan 10 22:14:00 bcron-scheduler[4198]: bcron-exec: (root) CMD (test -x /usr/lib/atrun && /usr/lib/atrun)
cron.info: Jan 10 22:15:00 bcron-scheduler[4198]: bcron-exec: (root) CMD (test -x /usr/lib/atrun && /usr/lib/atrun)
cron.info: Jan 10 22:15:00 bcron-scheduler[4198]: bcron-exec: (root) CMD (/sbin/sv once lta-push)
mail.info: Jan 10 22:15:00 dovecot: auth: passdb(lta-push,127.0.0.1,master): Master user logging in as
mail.info: Jan 10 22:15:00 dovecot: imap-login: Login: user=<, method=PLAIN, rip=127.0.0.1, lip=127.0.0.1, mpid=10121, TLS
mail.info: Jan 10 22:15:00 dovecot: imap(): Disconnected: Logged out bytes=409/2482
mail.info: Jan 10 22:15:00 dovecot: auth: passdb(lta-push,127.0.0.1,master): Master user logging in as
mail.info: Jan 10 22:15:00 dovecot: imap-login: Login: user=, method=PLAIN, rip=127.0.0.1, lip=127.0.0.1, mpid=10124, TLS
daemon.info: Jan 10 22:15:00 lta-push[10116]: done with LTA/10:0
mail.info: Jan 10 22:15:00 dovecot: imap(): Disconnected: Logged out bytes=585/2972
daemon.info: Jan 10 22:15:00 lta-push[10116]: 0 Messages Pushed for 2 user

fig. 42 protocol display

Part 2

UMA E-Mail-Client

8 UMA E-Mail-Client

The UMA E-mail client is the web interface for users. This client is for the administration for all received and sent e-mails, which are archived in the UMA. This UMA client is for three types of users.
For the normal user, who wants to get access on his archived e-mails with his own access code in a read-only mode.
Second Type is the auditor. This user is allowed to get access to the archives of the “normal users”, after he received the approval of the privacy officer (data protection commissioner).
The third type is the privacy officer. Auditor and privacy officer only can be named once on each appliance.

Every user is able to get logged in with his active directory registration code to see his e-mail account. You can see an inbox (all received e-mail), a sent box (place of all send e-mail) and the long term archives folder.
The user is able to search after e-mails; he can copy mails into other archive folders and is able to create personal filter setting. These settings allow that e-mails are placed additional in long term archive folders.

Note:
The lawfully authenticity is made by qualified time stamps and by the implementation of the specifications of the technical guideline 03125 of the BSI. This marking only happens in the long term files.

All data will be protected against unauthorized inspection from others by the “four-eyes-principle”. The auditor can use the e-mail-client-interface as Login into various accounts. In order to receive an unlimited access to UMA mail accounts, the auditor’s access must be confirmed by a Private Officer.
The auditor and the Private Officer will be registered on the administrators’ interface. This system only offers the necessary protection, if the auditor and the Private Officer are not the same person and the administrator proceeds conscientiously regarding their assignation.

8.1 Login

You enter the e-mail-client web interface over the internal IP address of the appliance.

- Type the hostname or the internal IP address of the appliance into the address field of your web browser. Use the HTTPS protocol.
  For example:

  ```
  https://my-uma.my-domain.com
  https://192.168.175.10
  ```

- If a security warning appears, assure that the used certificate is trustable. In this case confirm that you trust the certificate publisher. Add the certificate to the list of trustworthy certificates, if this functionality is offered by your browser.
- The e-mail-client web interface appears.
- Select the **user login**.

fig. 43 icon of the uder login

- Enter the **user name** of the active directory and use the according **password**.

fig. 44 UMA-mail-client login

8.2 Overview

After login to the user interface the personally user account opens. Here are shown all e-mails which are collected by the UMA in different folders. The start screen shows the content of the inbox.

fig. 45 sections and functions of the UMA e-mail client

8.3 Folder List

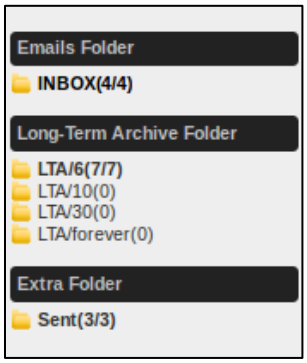

fig. 46 folder list on the left side

On the left side the folders **Inbox**, **Log Term Archives (LTA)** and **Sent** are listed.
The Inbox contains all e-mails which are received by the owner of this account. The send folder contains all sent e-mails. The LTA folders include the copies of the e-mails which are classified for archiving by the global filter rules. The global filter rules are defined by the administrator and are valid for all accounts.
You can set personal filter for your own account. These filters are only additional to the global filters.

8.4 E-Mail Filter

In this section filters can be adjusted which copy e-mails into the folders **6 years**, **10 years**, **30 years** or **forever**.
Several filters can be defined which can contain several conditions.
To set up a filter condition you have to enter a name for this rule first. Than you select the match conditions and the archive the matching e-mails should be copied to.

Match of conditions:

- **all rules match**
- **one rule matches**
- **no rule matches**

Following sections could be searched:

- **e-mail header**
- **e-mail body**
- **address**
- **body**

Note:

The section **body** includes the content of all attachments.

In dependency on the sections different conditions can be selected.

Section	Condition 1	Condition 2
e-mail header	subject / date	contains / matches / is
e-mail body	raw / content / text	contains / matches / is
address	to / from / carbon copy (CC)	contains / matches / is
size	greater than / less than	K / M / G (kilobyte / megabyte / gigabyte)

fig. 47 one e-mail filter with to conditions

Example:

All accounts, which are sent to customers should be copied to the LTA folder 10 (storage duration 10 years).

- Enter a name for the filter for example “sent accounts”.
- Because all following condition should be matched, select from the first dropdown field **all rules match**.
- From the second dropdown field select the desired LTA folder.
  For this example **LTA/10**.
- In the next row the first condition will be defined.
  Select **e-mail-header** as section.
  Define the exact section of the header and enter the term **subject**.
  As search mode select **contains** and type the word **account** into the filed.
- Click on the button with the plus symbol in front of the first condition to define a second one.
  This time select **address** as section.
- Select as limitation **from** out of the second dropdown filed and

as search mode **contains**.

Type your e-mail domain as text to search for.

Note:

Global filter settings set by the administrator take effect to all e-mail accounts. Filters which are defined in this section supplement the filter rules (see chapter 7.5).

8.5 Searching

You can search e-mails in to modes. Use the quick search to find an e-mail in the active folder. The search located in the main bar up to eight conditions can be defined.
The functions will be explained in the following chapters.

8.5.1 Quick Search

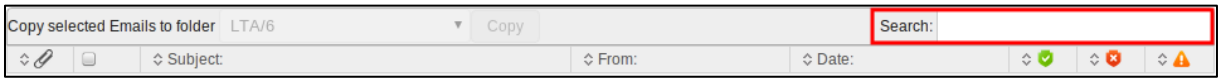

fig. 48 quick search field for the current folder

The quick search is located directly above the title bar of the e-mail list.
The searching is always limited to the current open folder.
From the second typed character the real time search will be executed. All e-mails the searching pattern applies to will be shown. All attributes shown in the list will be included.
You can narrow down the matches by extending the search pattern. The order of the pattern is irrelevant. So you can first search for a date and then limit the matches by entering a name.
For example:
Search pattern: **14/03 ado**

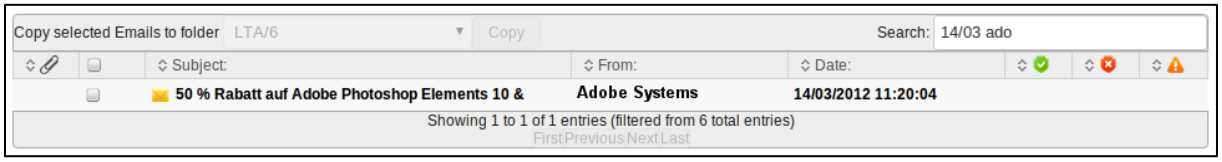

*fig. 49 result for search pattern **14/03 ado***

8.5.2 Advanced Search

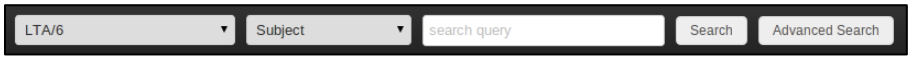

fig. 50 advanced search bar at the top of the client

The advanced search is located in the main bar of the client and can be activated by the button **Advanced Search**.
You can define the folder which should be searched and set up to eight conditions for the search. The conditions are composed of a **search group** and a **search pattern**.
If the search group is a date, the date must be selected from a calendar so the date is a single day. To search for an e-mail in a date range you have to set two conditions.
The text search will searched for words and word fragments in the selected section.
You can add and delete conditions by the buttons with the **Plus** and **Minus** symbol on it.
You can decide if all condition or just one has to match.

fig. 51 search for an e-mail from Fred Flintstone between the 1st and the 29th of February

8.6 Copy E-Mails

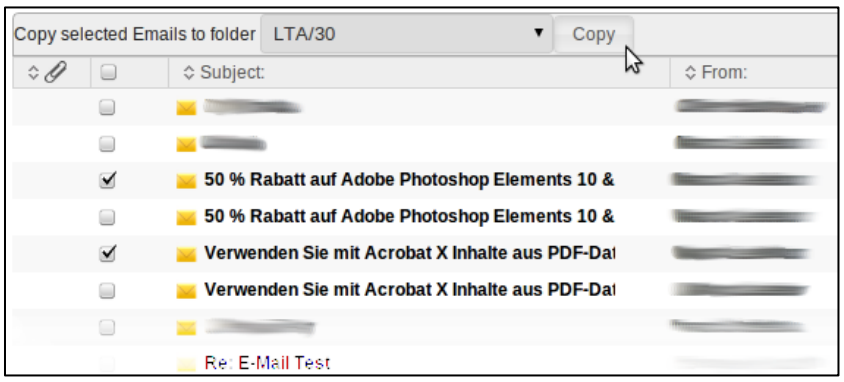
Copy selected Emails to folder
LTA/30
Copy
Subject:
From:
50 % Rabatt auf Adobe Photoshop Elements 10 &
50 % Rabatt auf Adobe Photoshop Elements 10 &
Verwenden Sie mit Acrobat X Inhalte aus PDF-Dat
Verwenden Sie mit Acrobat X Inhalte aus PDF-Dat
Re: E-Mail Test

fig. 52 copy two mails into LTA/30 folder

E-mails can be copied from one folder into another one. If you decide on a later date that accounts should be stored for 30 years and not only for 10 years, you can search the dependent e-mails and copy them into the according folder. The e-mails will be copied not moved.

E-mails with an activated checkbox in the second column of the table will be copied. If all e-mails should be selected or unselected, activate or deactivate the checkbox in the title bar of the list.

8.7 Display an E-Mail

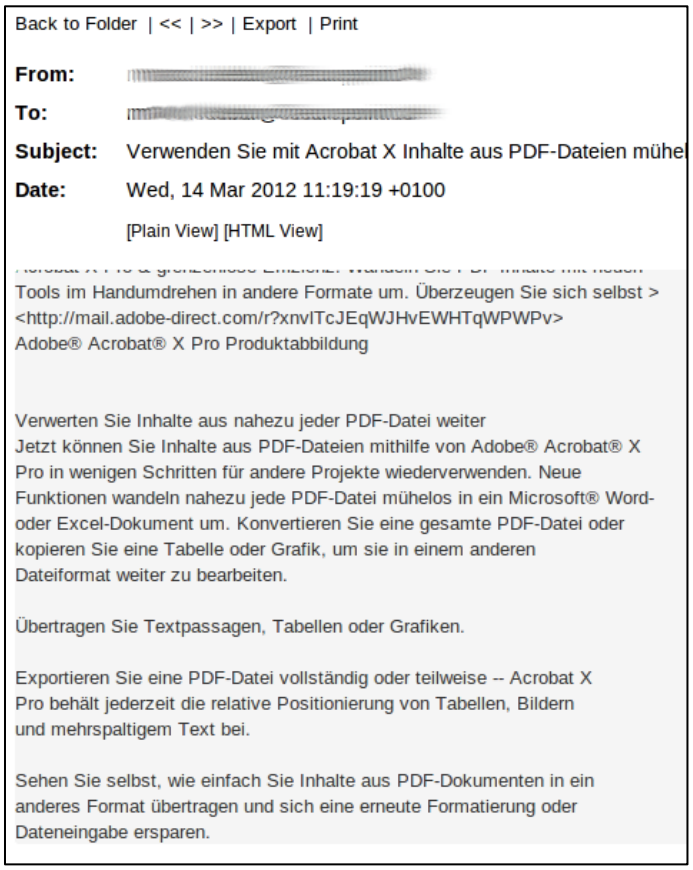
Back to Folder | << | >> | Export | Print
From:
To:
Subject: Verwenden Sie mit Acrobat X Inhalte aus PDF-Dateien mühel
Date: Wed, 14 Mar 2012 11:19:19 +0100
[Plain View] [HTML View]
Tools im Handumdrehen in andere Formate um. Überzeugen Sie sich selbst >
<http://mail.adobe-direct.com/r?xnvlTcJEqWJHvEWHTqWPWPv>
Adobe® Acrobat® X Pro Produktabbildung
Verwerten Sie Inhalte aus nahezu jeder PDF-Datei weiter
Jetzt können Sie Inhalte aus PDF-Dateien mithilfe von Adobe® Acrobat® X Pro in wenigen Schritten für andere Projekte wiederverwenden. Neue Funktionen wandeln nahezu jede PDF-Datei mühelos in ein Microsoft® Word- oder Excel-Dokument um. Konvertieren Sie eine gesamte PDF-Datei oder kopieren Sie eine Tabelle oder Grafik, um sie in einem anderen Dateiformat weiter zu bearbeiten.
Übertragen Sie Textpassagen, Tabellen oder Grafiken.
Exportieren Sie eine PDF-Datei vollständig oder teilweise -- Acrobat X Pro behält jederzeit die relative Positionierung von Tabellen, Bildern und mehrspaltigem Text bei.
Sehen Sie selbst, wie einfach Sie Inhalte aus PDF-Dokumenten in ein anderes Format übertragen und sich eine erneute Formatierung oder Dateneingabe ersparen.

fig. 53 display of an e-mail

By clicking on an e-mail in the list, it will be opened. The mail can be show in plain text or in HTML format. For switching the format use the buttons below the date.
Attachments of the e-mail can be downloaded by clicking on it.

Note:
To display Attachments you will maybe need according display programs on your system.

8.7.1 Navigation in Displayed E-Mails

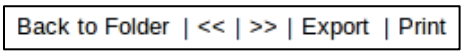

fig. 54 navigation bar in to of the shown e-mail

A navigation and function bar are placed above the displayed e-mail. Use this bar to navigate in the active folder and execute the export and print function.

Area / Field	Description
Back to Folder	Changes from the e-mail display back to the folder view of the active folder.
<<	Opens the e-mail which is located in the list in front of the current opened e-mail.
>>	Opens the e-mail which is located in the list behind the current opened e-mail.
Export	Exports the opened e-mail on to your system. If the e-mail contains attachments these will be exported too.
Print	The e-mail will be viewed in the print preview of your browser. Use the pint function of your browser to print the e-mail.

8.8 Inspection Report

As soon as an e-mail has been signed with the qualified time-stamp in a long-term archive folder, the e-mail will be marked with a green LZA icon in the list.
Click on this green icon to open the test report.

fig. 55 an inspection rport in german language

The long-term archive test report provides information about the qualified certificates used and the integrity of the electronic message. This also includes attachments. When an attachment has been signed adequately, before having been transferred into the evidence folder, also the author certificate and the attachment itself will be checked regarding identity and validity of signature at the point of time of installation.

The category **General Information** informs about the programme part of the UMA, which realizes the certificate inspection (name of report), at which point of time the test report has been compiled (created at), which version of test report is currently shown (version no.) and sums up the report result of all checked certificates (status).
The category **Archive time-stamp Sequence** demonstrates all test report results of the qualified time-stamps used.

Note:
The UMA works according to the technical directive 03125 of the “Bundesamt für Sicherheit in der Informationstechnologie” (Federal Office for security and information technology) in order to protect the used signatures by giving them an additional on-top-signature with the highest crypto logical algorithm by the MERKLE Hashbaum method. The qualified time-stamp is taken every day.

If the verified e-mail contains attachments, that have been signed adequately, the test results of the accepted certificates are shown in the category **Data Object Folder**.

9 Auditor Access

An auditor access can be defined in the administration web interface. The auditor can access every e-mail account if the privacy officer allows this access.

To prevent a misuse of this possibility the data are stored in four eyes principle. This means that the auditor cannot access to foreign e-mail account himself. After the auditor has to enter his login credentials the privacy has to approve the access by entering his own credentials.
The accounts of the auditor and the privacy officers are managed at the administration interface. The administrator has to ensure that the auditor and the privacy officer are not the same person.

9.1 Login as Auditor

- After opening the e-mail client web interface of the UMA the supervisor mode has to be selected.

fig. 56 icon of the auditor login

- The mask for the external auditor login appears.
- The auditor has to enter the user name and the password into the according fields. These credentials are not the Active Directory credentials.
- After successful login the e-mail account which should be shown has to be selected from the dropdown list.
- The privacy officer enable the access to the selected e-mail account by enter his credentials.

The auditor now has access to the selected e-mail account. The auditor can use the search, the print and the print functions.
No e-mail filter can be set and nor e-mails can be copied into other folders.

When the user opens his account the next time a message appears that an auditor has accessed the account since his last login.

Part 3

affix

10 Change the IP Address in Windows 7

In delivery status the IP address of the appliance is set to 192.168.175.245. If you connect the appliance with the network, you can only access the appliance if your computer has an IP address out of the subnet 192.168.175.0.

For Microsoft Windows 7 follow these instructions. For these settings you will need administrator rights.

- Click on **Start** (the Windows icon in the left bottom corner).
- Select the **Control Panel** from the **Start Menu**.
- Select the group **Network and Internet** in the appearing dialog.
- Select the group **Network and Sharing Center** in the new dialog.
- On the left side of the window you will find the entry **Change adapter settings**.
- Select **active LAN connection** and click on it with the **right mouse button**.
- Click on the entry **Properties** in the **context menu**.
- The dialog **Local Area Connection Properties** appears.
- Select the entry **Internet Protocol Version 4 (TCP/IPv4)** in the middle window with the title **This connection uses the following items**.
- Click the button **properties** below this window.
- Click the button **Advanced…** in the new dialog.
- A new window appears. Switch to the tab **IP Settings**. Click on **Add…** at the area **IP addresses**.
- The mask **TCP/IP Address** appears. Enter an IP from the subnet **192.168.175.0** into the field **IP address** (for example 192.168.175.11).
- When you switch to the field **subnet mask** this will be filled with 255.255.255.0. You can keep this.
- Click on **Add**.
- Close the other dialogs with **OK**.

11 Create a HUB E-mail Account on a MS Exchange Server

The following shows briefly, how to create a HUB account on a Microsoft Exchange Server. This article offers just a short overview. For further information read the MS Exchange documentation.
The screenshots are made from a Microsoft Server 2008 R2 with service package 1.

11.1 Define Authentication Method of the IMAP Server

The “Plain Text Logon” without TLS connection must be activated for logon.
The “Secure Logon” is set by default.

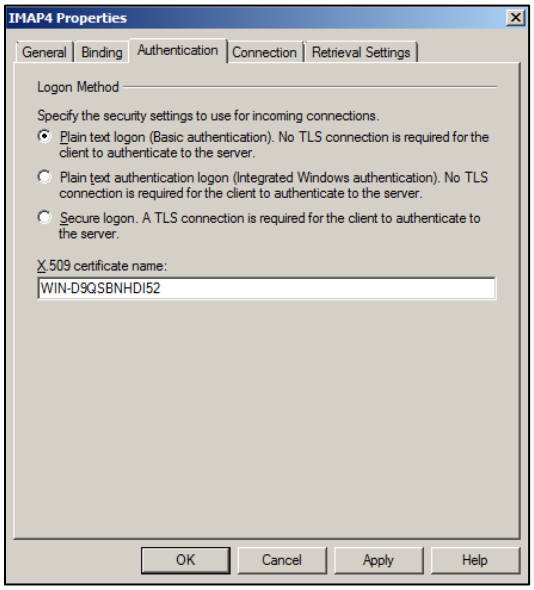
IMAP4 Properties
General
Binding
Authentication
Connection
Retrieval Settings
Logon Method
Specify the security settings to use for incoming connections.
Plain text logon (Basic authentication). No TLS connection is required for the client to authenticate to the server.
Plain text authentication logon (Integrated Windows authentication). No TLS connection is required for the client to authenticate to the server.
Secure logon. A TLS connection is required for the client to authenticate to the server.
X.509 certificate name:
WIN-D9QSBNHDI52
OK
Cancel
Apply
Help

fig. 57 change logon method

- Open the **Exchange Management Console**.
- Select the item **Client Access** from the left tree structure **Server Configuration**.
- In the bottom window in the middle show the entries **IMAP4** and **POP3**.
- Click right on **IMAP4** and select the context menu point **Properties**.
- Switch to the tab **Authentication** and select the first entry: **Plain Text Logon (Basic Authentication)**.

11.2 Change the Start Type of the Service

The service must be restarted for the change of the authentication method takes effect. Furthermore the service should start automatically.

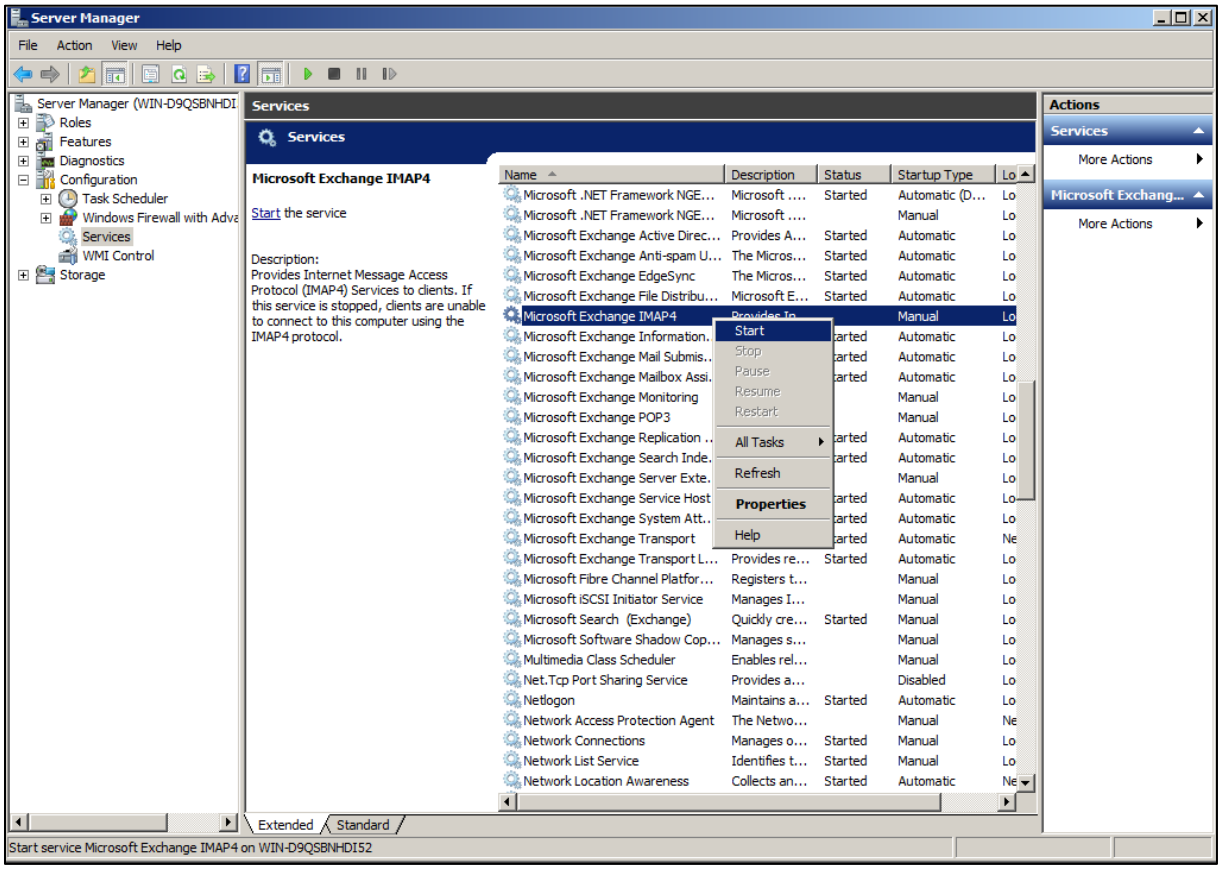

fig. 58 start IMAP4 service

- Open the **Server Manager**.
- Select the item **Services** form the tree structure point **Configuration**.
- Select the item **Microsoft Exchange IMAP4** from the list. Open the context menu by clicking on this item with the right mouse button.
- Click on the entry **Start** to start the service.

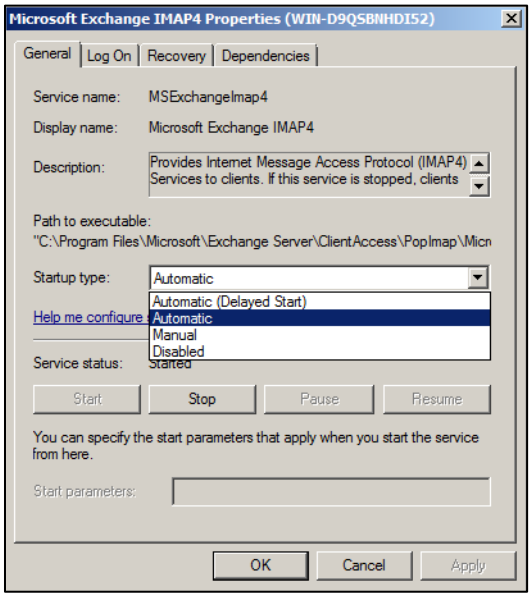

fig. 59 set start type to "automatic"

- Activate the context menu of the entry **Microsoft Exchange IMAP4** a second time.
- Click on the item **Properties**.
- Switch to the tab **General**. Select from the dropdown menu **Start type** the item **Automatic**.
- Click **OK**.

11.3 Exchange Management Console

Open the Exchange Management Console in the administration interface of your server system.

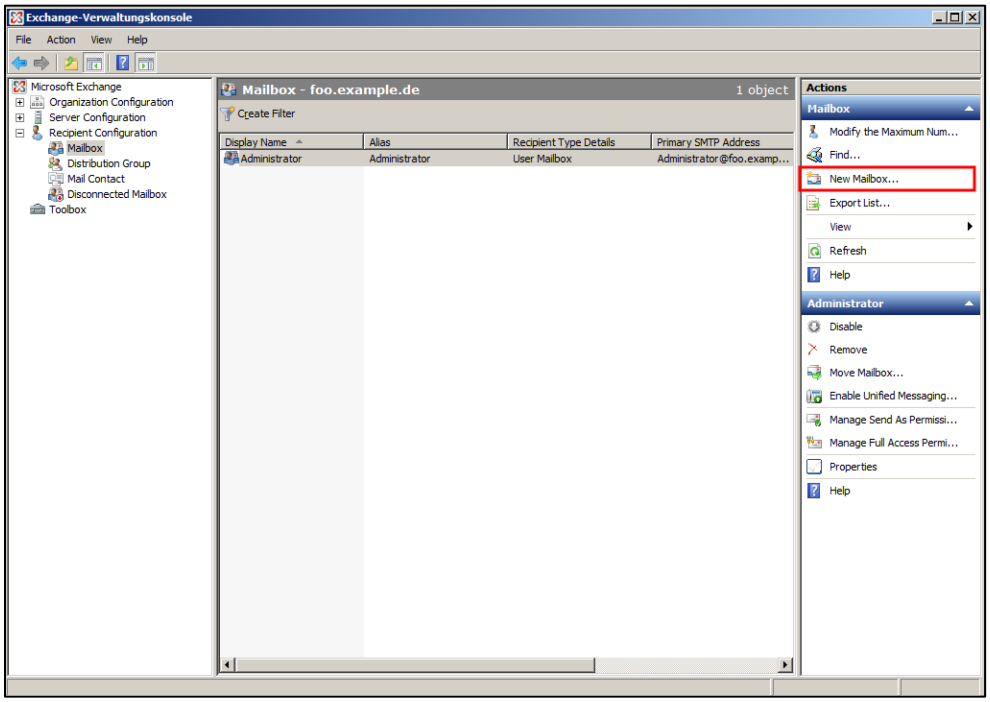

fig. 60 Exchange Management Console

- Switch in the left tree structure to the item **Recipient Configuration** sub item **Mailbox**
- Click on the item **New Mailbox** in the right window named **Actions**.
- The **Mailbox Wizard** appears.

The wizard guides you through the several steps of creation a new mailbox.

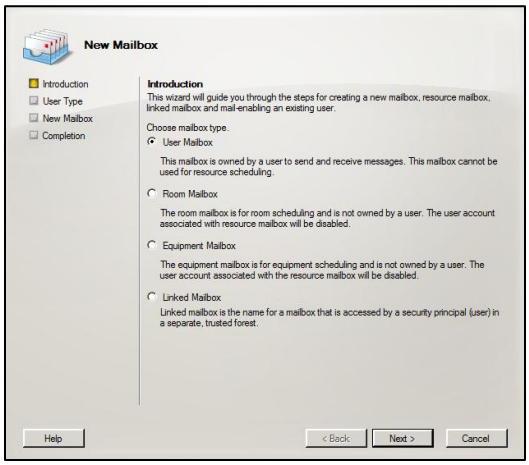
New Mailbox
Introduction
User Type
New Mailbox
Completion
Introduction
This wizard will guide you through the steps for creating a new mailbox, resource mailbox, linked mailbox and mail-enabling an existing user.
Choose mailbox type.
User Mailbox
This mailbox is owned by a user to send and receive messages. This mailbox cannot be used for resource scheduling.
Room Mailbox
The room mailbox is for room scheduling and is not owned by a user. The user account associated with resource mailbox will be disabled.
Equipment Mailbox
The equipment mailbox is for equipment scheduling and is not owned by a user. The user account associated with the resource mailbox will be disabled.
Linked Mailbox
Linked mailbox is the name for a mailbox that is accessed by a security principal (user) in a separate, trusted forest.
Help
< Back
Next >
Cancel

fig. 61 select mailbox type

- Select the radio button **User Mailbox** as account type.
- Click **Next >**.

A mailbox can be created for an existing user or for a new user. We create a new user for the Hub mailbox.

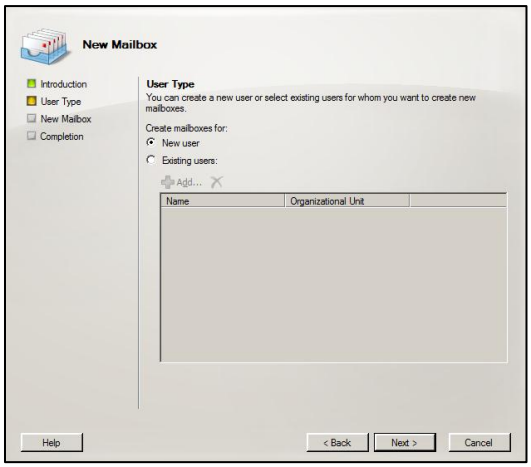

fig. 62 select user

- Select the radio button **New User**.
- Click **Next >**.

The next step queries the user information of the new user.

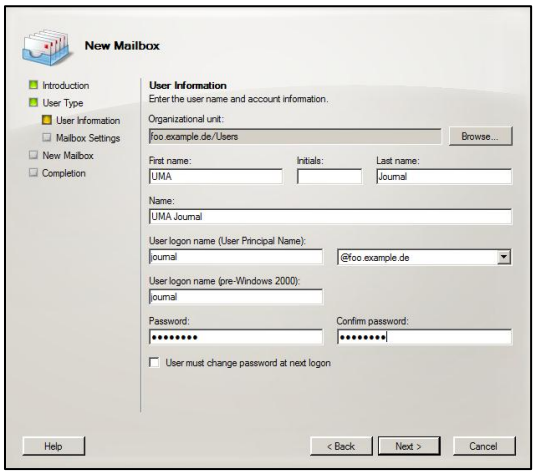

fig. 63 enter user information

- Enter the **Organization unit** of the user. Use the button **Browse…** and select the unit in the appearing dialog.
- Enter the **Last name** and the **First name** of the user.
- Define the **User logon name** and the **Password**. Confirm the password by retyping it.
- Click **Next >**.

In the next step enter the alias of the user.

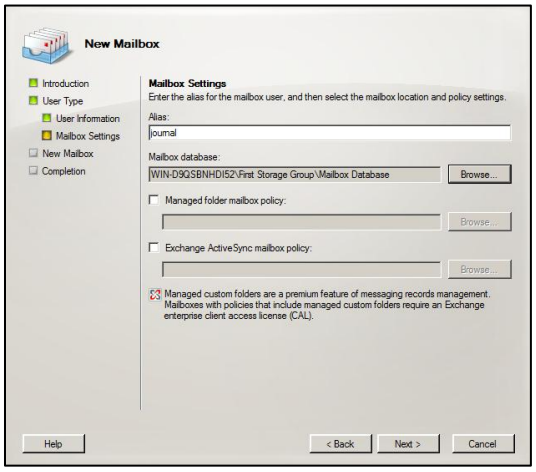
New Mailbox
Introduction
User Type
User Information
Mailbox Settings
New Mailbox
Completion
Mailbox Settings
Enter the alias for the mailbox user, and then select the mailbox location and policy settings.
Alias:
journal
Mailbox database:
WIN-D9QSBNHDI52\First Storage Group\Mailbox Database
Browse...
Managed folder mailbox policy:
Exchange ActiveSync mailbox policy:
Managed custom folders are a premium feature of messaging records management. Mailboxes with policies that include managed custom folders require an Exchange enterprise client access license (CAL).
Help
< Back
Next >
Cancel

fig. 64 select alias name and storage location

- Select the storage location of the mailbox in the field **Mailbox database**.
- Click **Next >**.

A summary of the properties of the new account is shown.

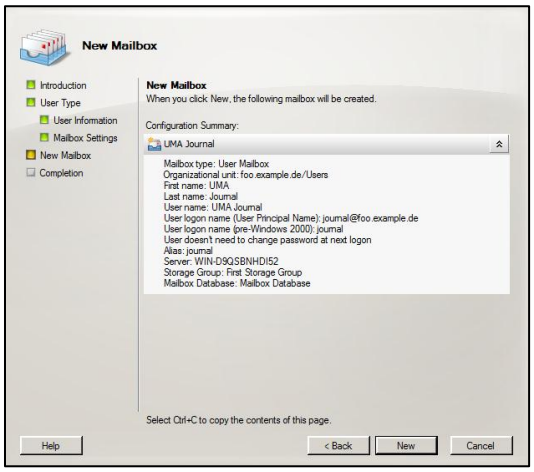

fig. 65 summary

- Check all selected item and approve the creating of the account by clicking **New**.

The wizard shows the result of the creation.

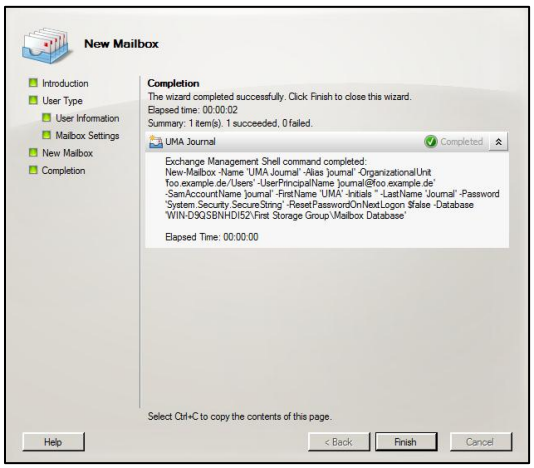

fig. 66 mailbox created successfully

- Close the wizard by clicking **Finish**.

You will be directed back to the Exchange Management console.

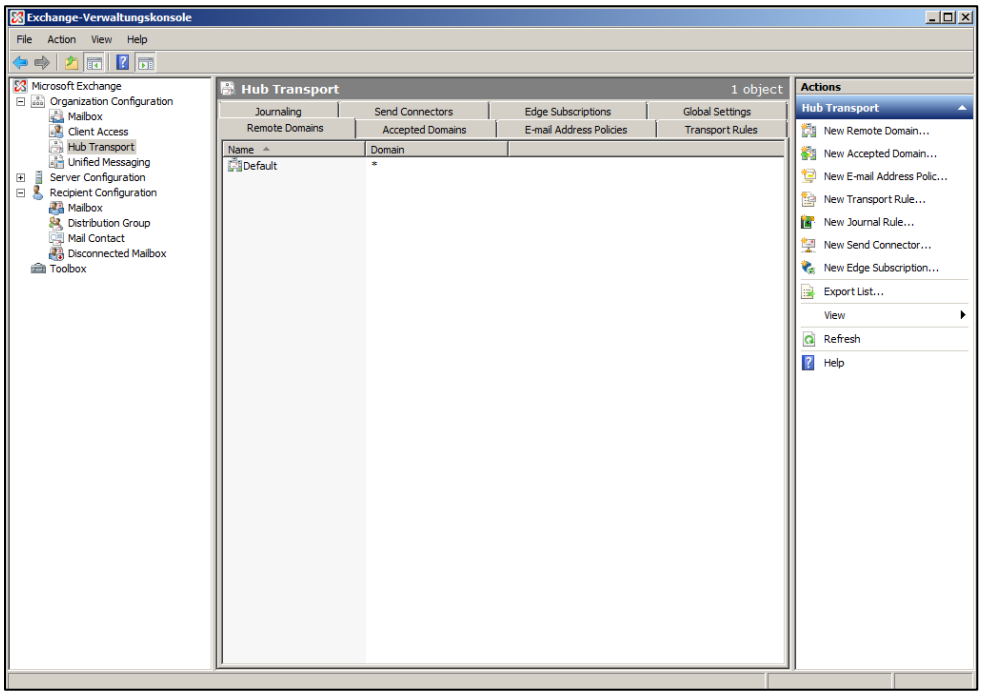

fig. 67 Exchange mangement console - Hub Transport view

- Click under **Organization Configuration** on **Hub transport** in the left tree structure.
- Click in the right window actions on **New journal rule…** .

The dialog New Journal rule will be opened.

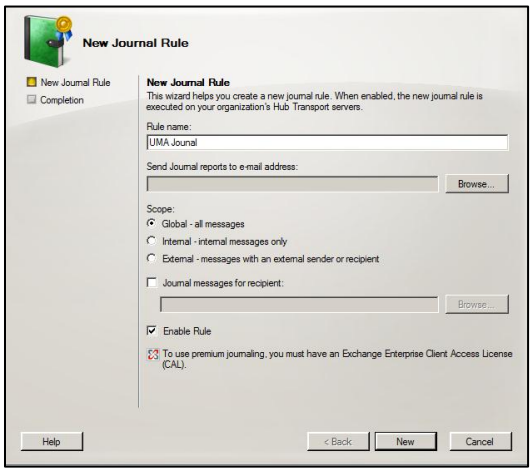
New Journal Rule
New Journal Rule
Completion
New Journal Rule
This wizard helps you create a new journal rule. When enabled, the new journal rule is executed on your organization's Hub Transport servers.
Rule name:
UMA Journal
Send Journal reports to e-mail address:
Browse...
Scope:
Global - all messages
Internal - internal messages only
External - messages with an external sender or recipient
Journal messages for recipient:
Browse...
Enable Rule
To use premium journaling, you must have an Exchange Enterprise Client Access License (CAL).
Help
< Back
New
Cancel

fig. 68 set name for journal rule

- Enter a name for the new rule into the field rule **name**.
- Click **Browse…** beneath the field **Send Journal report to e-mail address**.

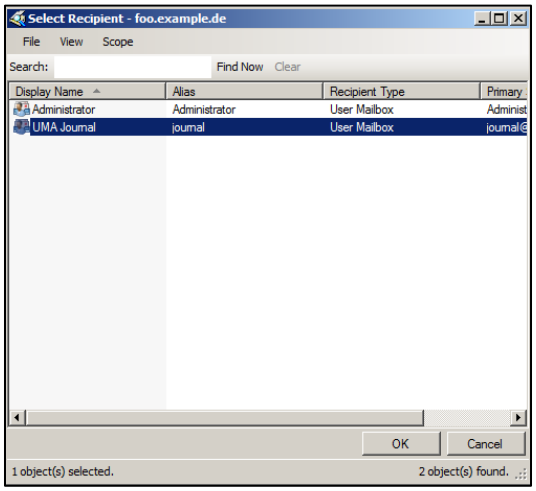

fig. 69 select recipient

- Select the **new created user** as recipient in the appearing window.
- Click **OK**.

You have to define which messages should be copied to the Hub account.

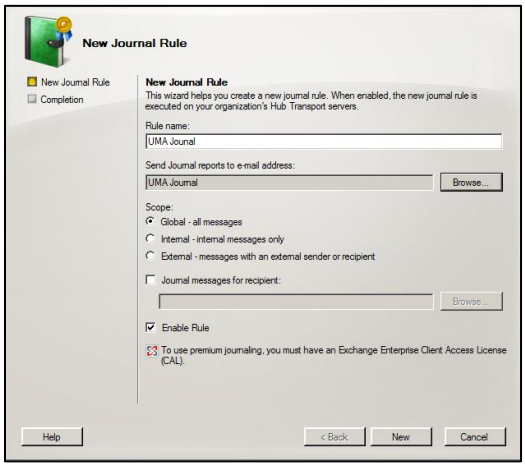
New Journal Rule
New Journal Rule
Completion
New Journal Rule
This wizard helps you create a new journal rule. When enabled, the new journal rule is executed on your organization's Hub Transport servers.
Rule name:
UMA Journal
Send Journal reports to e-mail address:
UMA Journal
Browse...
Scope:
Global - all messages
Internal - internal messages only
External - messages with an external sender or recipient
Journal messages for recipient:
Browse...
Enable Rule
To use premium journaling, you must have an Exchange Enterprise Client Access License (CAL).
Help
< Back
New
Cancel

fig. 70 select messages and activate rule

- Select the radio button **Global – all messages**.
- Activate the checkbox **Enable Rule**.

A summary of the selected settings and the result of the creation is show in the last window.

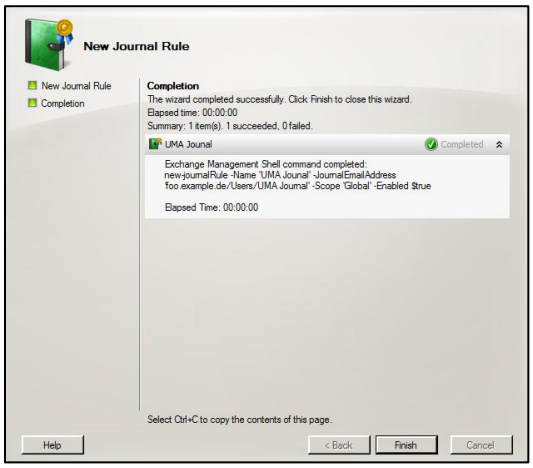

fig. 71 rule created successfully

- Check the summary and click **Finish**.

All e-mails will be copied into the new mailbox.

If the UMA is configured in Hub mode all e-mails will be fetch from this mailbox.

After the e-mails are fetched from the hub mailbox they can be deleted.